ISSN 2395 2733

Sardar Vallabhbhai Patel National Police Academy Journal

Vol. LXXIV, No. 2
DECEMBER, 2025

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

December, 2025

Vol. LXXIV, No. 2

Published by
SVP National Police Academy
Hyderabad

ISSN 2395 2733

SVP NPA Journal

December, 2025

EDITORIAL BOARD

Contents

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P. 1-14)

Countering the Threat of Drones – Challenges and Solutions

Jose Mohan, IPS*

Keywords

Threats from Drones, Counter Unmanned Aerial Systems (C-UAS), Challenges, Legal implications, Interdiction hazards, Counter Drone Solutions, Synergy, Precautions, Responsibility to counter the threat.

1.0 Introduction:

From entertainment to logistics, and security operations to agriculture, drones strengthen the sophistication as well as developmental activities in various sectors of the economy. But, with the potent nature of Unmanned Aerial Systems (UAS), it poses a serious threat to public safety and national security. It may be the easiest tool to maximise the damage which could be inflicted on the strategic installations of a country. UAS is also a formidable tool for committing crime and it could be used to commit wide range of crimes viz. theft, smuggling, espionage, rioting, hacking, attacks and even murder. Besides this, the issues created by the negligent drone fliers brings a whole set of new challenges.

The emerging threat spectrum of drones is highly dynamic, and the disruptive aspect of the technology is fast evolving. Without waiting for the threat to become a reality, the counter drone mechanism must be matching with the threats. The responsibility to prevent crime and security incidents primarily reside with the police forces of the country. Hence, the

* *Central Industrial Security Force (CISF) as Inspector General*

police forces need to be prepared and equipped to face the challenges posed by this evolving threat.

The first part of this article will be examining various dimensions of threat from drones, concept of counter drone measures and challenges posed by the drone technology. In the second part, counter drone solutions, factors bringing synergy, precautions while deploying ADS and finally, the responsibility to counter the threat from drones are discussed. The effectiveness of Anti-Drone Systems (ADS) is dependent on complex and multitude of factors and because of this, a holistic as well as integrated design considering all component factors is required. This paper will conclude by stating that effectively countering the threats from drones requires a strategic approach with risk management, layered defence and resilience plan.

2.0 Threats from drones:

Threats in the context of UAVs may be defined as an impending danger from drones that has the potential to cause fear in the minds of people, harm to the life, damage to the property or disruption of systems. Drones are considered as one of the most potential contemporary disruptive technologies and it have become increasingly accessible due to reduction in cost, advancements in technologies and ease of operations. Hence, the threat from drones is also getting expanded. Nation-states, non-state actors, criminals, smugglers, and even untrained hobbyists are exploiting these aerial systems for activities that challenge public safety and internal security.

Terrorist Organisations and extremist groups use drones for many subversive activities viz. to distribute the propaganda materials, to gather actionable intelligence, target acquisition, delivery of prohibited items viz. drugs and narcotics, weapons, currencies and other contraband items[2]. It gives an easy medium of transportation, delivery, distribution and execution for militant organisations.

Among various critical sectors, aviation sector is most vulnerable both from negligent drones as well as targeted attacks, and the threat from drones to aviation sector is a reality. An incursion drone, malicious or

negligent can have serious security, safety and economic impact on airport operations[5]. In India, for the year 2024 and 2025, there were a total of 165 incidents of drone sightings which were reported from various civil aviation airports in the country. Among the list, IGI airport New Delhi reported the highest. It is interesting to note that among these a good number of drones were noticed by the pilots of the aircraft or detected by the security personnel with naked eye [8].

Even though aviation sector is highly vulnerable, the impact of damage may be much higher in other sectors like atomic energy and oil facilities. The extent of damage caused by drone attack in Aramco oil facilities (2019), Saudi Arabia was enormous. The attack resulted in massive fire and disrupted production of about 5% of the world's oil supply, leading to a significant spike in global oil prices.

Figure-1: Massive fire after the drone attack at Aramco Oil Facility, Saudi Arabia

Further, the capability of drones as a potent weapon is evident from the incidents of drone attacks on the President of Venezuela, Prime Minister of Japan and Chancellor of Germany [8].

Another important installation which is highly vulnerable to the misuse of drones is the Prisons. Drones can completely negate the security set up in the jails and it can get in and out of the jail premises quite quickly much before the traditional response from security agencies [7]. In the year 2023, the prisons in England and Wales recorded 1,063 drone sightings which is

more than double the sightings in 2022, bringing drugs, mobile phones, other communication gadgets, incendiary devices, weapons and so on [7].

Figure-2: Delivery of restricted items using drones.

3.0 Concerns and Challenges from the Drone Technology:

The integration of various technologies along with miniaturisation in the field of drones are accelerated by the Artificial Intelligence (AI) and Machine Learning (ML). May be on the same pace or even at a faster rate, the disruptive nature of technology is transforming. However, the field of Anti-Drone Systems (ADS) is struggling to catch with the challenges thrown by the breakthrough innovations. Some of the important concerns to counter the threats from drones are summarised below.

3.1 Advancements in the communication and navigation technologies: Use of 5G communication in drones, frequency hopping, use of unauthorised frequency bands, autonomous drones mostly with highly unpredictable flight paths, UAVs that operate in GNSS denied environments, and use of unconventional navigation create challenges to the counter UAS (C-UAS) solutions. 5G drones cannot be normally detected using RF detection techniques and it could be remotely controlled from far-away places. Many a time, it is quite a challenging task to locate the actual operator especially in the case of 5G drones. Drones from hostile countries are often equipped with anti-jamming frequency hopping or stealth capabilities. Advanced GNSS receivers in drones are also increasingly being designed to reduce

interference from the ground, which makes it difficult to jam or spoof using terrestrial systems. UAVs are also being developed with features to detect incoming spoofing attacks.

3.2 Stealth and tethered drones: RF silent drones which are made of materials that reduce radar visibility is quite difficult to detect. The fibre optics tethered drones which are immune to all kinds of jamming are proven to be one of the most dangerous weapons in the ongoing Russia – Ukraine war. The range of these tethered drones are even up to 50 kms making the entire international border highly vulnerable.

3.3 Technological limitations of ADS: The technological solutions are evolving and none of the technology could be categorised as zero error. For example, radars and EO systems may fail to detect small drones, and it may get confused with other flying objects or birds. Moreover, these systems require direct line of sight for effective detection. "Electro-magnetic interference can degrade the detection capabilities of RF sensors. In urban environments, there are many potential sources of such interference, including communications antennae, two-way radios, telemetry systems, and even power lines and LED lights"[9].

3.4 Response time: The availability of time to respond to a drone attack or incursion of a rogue drone is very low. So, the counter drone technology needs to be quick with high level of automation and decentralised decision making. There needs to be a robust framework and well established standard operating procedures to empower the personnel at the ground level to take quick decisions.

3.5 Lack of standards: "No international or national standards exist for the proper design and use of C-UAS systems. This means there may be significant variances between the performance and reliability of systems that might, at the spec-sheet level, appear to be very similar". In the C-UAS industry, "many firms appear to be working to capitalize on the growing interest in this technology before properly maturing or field-testing their products" [6]. Further, it is reported that "a large proportion of systems that are actively marketed to government customers do not perform as advertised" [6]. The absence of standards creates confusion, non-compliance and raises issues of safety.

3.6 Legal implications: The use of C-UAS is often subject to numerous overlapping laws that were drafted long before counter-drone technology existed [6]. Legal implications in C-UAS may include non-compliance of the existing laws / guidelines, issues related to misuse of C-UAS technologies, data protection, unauthorised use of wireless technologies in ADS, use of restricted gadgets, obstruction / jamming of different bands in the electromagnetic spectrum, use of powerful lasers, legal protection from damage to life and property during the use of ADS etc. There needs to be a legal framework allowing police to intercept drones by force, including disturbing the connection between the drone and its operator [6].
3.7 Counter-drone technology is often very expensive, arbitrary, and most manufacturers do not disclose their price lists.
3.8 Personnel training, maintenance, and adequate staff to operate the counter-drone system is also required.
3.9 Interdiction hazards: The use of ADS is likely to cause collateral damage during its operations. Both kinetic and non-kinetic measures have the risk of damaging unintended nearby objects, infrastructure, or injuring people on the ground because of the countermeasure itself or the falling drone debris.
3.10 Improper use of C-UAS raises troubling concerns around safety, legality, privacy, coordination, planning, and airspace integration [6].

4.0 Counter Drone Solutions:

Solutions to counter the threats from drones are technological together with non-technological, and both synergises one another. Technological solutions refer to the systems designed to detect, track, identify, intercept and/or neutralise UAVs particularly small drones that cannot be countered with traditional anti-aircraft systems designed for use against manned aircraft [9]. Non technological solutions include various preventive and protection methods.

The preventive measures may include installation and operationalisation of ADS, standardisation of procedures, intelligence gathering, awareness campaigns, regulatory guidelines, penal provisions on non-compliant drones for deterrence, zonal restrictions of drones,

geofencing, licencing, restrictions on manufacture, import, sale, and use of drones etc [8]. Protective measures include various target hardening measures, additional layer of physical security and so on. Camouflaging the vital assets is extremely helpful to protect it from attacks. Netting is an effective protective measure, and it could successfully protect strategic assets and vital installations to a greater extent. Netting over fuel farms, ATC, other critical assets protect from access of drones [10]. In the case of prisons, netting functionally prevents the delivery of contrabands, weapons and restricted items inside the prison.

Figure-3: Netting to protect critical systems

Figure-4: Netting to protect fuel storage tank.

Drone monitoring and neutralisation are the technological solutions to counter the threats from drones. Drone monitoring equipment can be passive (simply looking or listening) or active (emitting a signal and analysing what comes back), and can perform several functions viz. detection, classification or identification, locating and tracking, alerting etc. It includes radars of various capabilities, Radio Frequency (RF) detection, Electro-Optic (EO) multi-spectrum cameras, acoustic detection, other sensors, cyber detection and analysis etc [8]. Multi sensor approach with live feeds to an integrated command and control centre capable of alerting and coordinating helps in a comprehensive detection and decision-making.

Classification of drones helps to segregate drones from birds and other flying objects in the sky. One step further is identification, which identifies whether the drone is Bonafide one or not, model of the drone, protocol being used and controller's fingerprint like MAC address. Identification relies not only on electronic signatures but also on factors such as flight behaviour, location, payload indicators, and operator proximity. Tracking gives the location of the drones in real time thereby enhancing the situational awareness and neutralisation capability[8]. With the advancements in data analytics and AI, the capabilities of monitoring techniques have gone up substantially.

Drone neutralisation techniques also seen a considerable improvement in the past few years especially with the integration of monitoring techniques with kill options. The kill options include non-kinetic and kinetic solutions. The non-kinetic mechanisms include jamming (both RF communication link and GNSS), use of high-power microwaves [3], directed energy systems, dazzling, laser guns, spoofing techniques, cyber takeover solutions etc. The kinetic solutions include use of projectiles, firearms and ammunition, collision systems, net catchers, drone on drone techniques etc.

Notwithstanding the above technological advancements, it may be relevant to state that in the absence of technological solutions, the most common method of detection is visual detection through the naked eyes followed by acoustic detection through the ears. Further, the neutralisation

method could be as crude as conventional common man's weapon like stone, lathi or a long stick, depending upon the situation.

Even though, there are many counter drone systems, there is no single solution which can fit into all security situations. The counter drone solution must be decided depending upon the conditions, place where it has to be deployed, total risk, threats, vulnerabilities and the budget. In a holistic perspective, it could be stated that the counter drone technology is only a part of the counter drone solution, and the preventive as well as protective measures to counter the threats are equally important.

5.0 Synergy of Counter drone solutions:

5.1 Know your enemy: In order to operationalise an effective counter drone solution, there must be a deep understanding of the type of drones, its capabilities, strengths and weaknesses. Knowledge about the intent and strategy of the operator are equally important. The skill of the counter drone operator in drone flying is also important.

5.2 Integration of technologies: Selection of counter drone technology and gadget depends upon the threat and features of the location where the ADS is to be installed. Deployment of counter drone gadgets by other establishments in the area also needs to be considered. Based on this a decision needs to be taken about integration of different counter drone equipment and technologies to bring harmony. Integration of detection and neutralisation technologies with the command-and-control centre of the city / establishment is critical to get synergy.

5.3 Layered defence: A layered approach deploys multiple, complementary technologies in a sequence to prevent, detect, track, identify and neutralize threats, from long-range detection to close-in physical defence. This strategy mainly combines various detection technologies and neutralisation options to create overlapping protections against threats.

5.4 Trained Personnel: Effective drone policing requires much more than technological solutions and preventive measures. The skills set and understanding of the counter drone equipment operators are paramount. It demands trained personnel who understand drone behaviour, technology

performance parameters, legal provisions, operational risks, and tactical response. The complexities of drone operations involve interpreting sensor data, analysing threat indicators, making split-second decisions, and deploying neutralisation assets under pressure. Police personnel must therefore undergo specialised training in drone operations, drone detection systems, electronic warfare principles, cyber intrusion techniques, drone forensics, and rapid-response tactics. The threat environment changes rapidly, necessitating continuous capacity building that keeps pace with evolving drone technology.

5.5 Institutional coordination: This may be considered a cornerstone of drone policing as no single agency can manage the entire threat spectrum. Lack of coordination among agencies is bound to be counter-productive in counter drone operations.

6.0 Precautions while deploying Anti-Drone Systems:

6.1 Regulatory Compliance: The anti-drone technology and solutions shall be procured, installed, deployed, used and maintained in compliance to the extant rules and guidelines issued by the government time to time.

6.2 Coordination: The ADS deployment and use shall be in coordination with sister agencies in the nearby areas to avoid disruption of ADS systems. Jamming or higher energy levels of the EM waves used by one agency may reduce the detection capabilities of ADS deployed by another agency.

6.3 Right Systems based on the threat: The ADS deployment shall be according to the suitability and requirement to the location and purpose to which it is deployed. Careful choice shall be made about Type I, II and III systems.

6.4 Interference: The interference to the existing communication and navigation systems shall be considered. Deployment and use of ADS near an aerodrome shall be in consultation / coordination with ATC of the aerodrome.

6.5 Interdiction hazards: Once the mitigation system is activated, depending on the technique used, this could result in a range of effects including the drone landing on the ground or activating a ‘return to home’,

the capture of the drone (nets), or the complete or partial destruction of the drone[6]. The drone may abruptly fall causing injury, damage or destruction. Depending upon the neutralisation measures, necessary precaution shall be taken to prevent injury or loss of life, and damage or destruction of property.

6.6 "Depending on the circumstances, once a drone is intercepted the device may need to be isolated and retrieved. If the drone is potentially armed, an explosive ordnance disposal team may be called in to assess and, if needed, disable the device. Unarmed drones must likewise be treated with caution. If the device is damaged, its lithium-ion battery poses a risk of combustion. If the device continues to be functional, its rotors can pose a risk of injury". For forensic analysis on the device, ensure that the integrity of the system and the potentially valuable data it carries are not compromised [6].

7.0 Responsibility to Counter the Threat from Drones:

Ministries of the Government of India are responsible for policy formulation, licensing, regulation, and authorisation of counter-drone measures. The responsibility of defence forces is mainly in accordance with the union war book and as per the orders issued by the Ministry of Defence / Ministry of Home Affairs in this regard. State governments oversee implementation especially in urban policing, event security, and critical infrastructure protection. Intelligence agencies contribute through threat profiling, monitoring hostile entities, and analysing emerging patterns.

At the ground level, the professional responsibility to protect the citizens, their safety and security is mainly with the police forces of the country. Moreover, almost all counter drone technologies involve use / interception of unlicenced / licenced electromagnetic waves, or use of restricted gadgets of strategic importance, prohibited firearms/weapons, or use of force which could be done by the State only. If there is a drone incident, the responsibility to investigate, undertake forensics and prosecute will also be with the government / police forces. However, policing drones involve intricacies of technologies and high level of

coordination. Internationally, the blurring of roles between Aviation Administration Authorities and the police in countering the rogue drones is widely accepted [1]. In short, the responsibility to protect the people, vital installations and border of the country from non-military grade drones up to a height of 120 metre in the airspace rests primarily with the police force responsible to protect it. For example, in the international border, the responsibility of first responder is with the border guarding forces, vital installations by the force responsible to protect it, VVIP by the agency assigned with the task to protect the VVIP and state police concerned in their respective areas. The first responder for the airspace above 120m AGL is the Indian Air Force [8].

8.0 Conclusion:

The threat from drones is real and adoption of counter drone solutions has to be matching with the advancements in the drone technology. To effectively counter the threats from drones, there must be a strategic approach with risk management, layered defence and resilience plan. The layered approach may include prevention, protection, various techniques of detection and neutralisation. The path forward is balancing technological advancements with legal and ethical considerations, building a proactive, structured, and technologically empowered policing ecosystem capable of securing India's skies. With sustained investment, coherent policy frameworks, and dedicated operational capacity, policing in India can meet the demands of the drone era with confidence and competence.

References:

1. *Fox, Sarah Jane. (2019, March 01). Policing: Monitoring, Investigating and Prosecuting 'Drones'. European Journal of Comparative Law and Governance. Brill, Netherlands. https://brill.com/view/journals/ejcl/6/1/article-p78_78.xml*
2. *Henschke, Adam; Reed, Alastair; Robbins, Scott & Miller, Seumas.(2021). Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism. Advanced Sciences and Technologies for Security Applications. Springer Nature,Germany.*

https://library.oapen.org/bitstream/handle/20.500.12657/52393/1/978-3-030-90221-6.pdf#page=16

3. *Kallenborn, Zachary & Plichta, Marcel. (2024, July 15). Breaking the shield: Countering Drone Defenses. National Defense University Press, Washington, DC.https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3838997/breaking-the-shield-countering-drone-defenses/#:~:text=Radio%20frequency%20and%20GNSS%20jammers,to%20locate%20the%20correct%20signal.*
4. *Lykou, Georgia; Moustakas, Dimitrios & Gritzalis, Dimitris.(2020, June 22). Defending Airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. MDPI, Switzerland. https://www.mdpi.com/1424-8220/20/12/3537*
5. *Markarian, Garik & Staniforth, Andrew. (2020, November 30). Counter measures for aerial drones. Artech House, Boston. https://us.artechhouse.com/Countermeasures-for-Aerial-Drones-P2065.aspx*
6. *Martins, Bruno Oliveira; Michel, Arthur Holland & Silkoset, Andrea. (2020). Countering the Drone Threat Implications of C-UAS technology for Norway in an EU and NATO context. Peace Research Institute Oslo (PRIO). Norway. https://www.researchgate.net/profile/Bruno-Martins-4/publication/348189950_Countering_the_Drone_Threat_Implications_of_C-UAS_technology_for_Norway_in_an_EU_and_NATO_context/links/5ff3240492851c13feeb0e08/Countering-the-Drone-Threat-Implications-of-C-UAS-technology-for-Norway-in-an-EU-and-NATO-context.pdf*
7. *Moore, Ben & Bish, Alex. (2024, November 26). Drones could bring in more 'risky' items to prison. BBC. https://www.bbc.com/news/articles/cr4lk0g96zpo*
8. *NPM Division of BPR&D. (2025, Novemeber 17). Project Report:"Solutions to counter threats from drones and establishment of CRD unit for Police/CAPFs". BPR&D(MHA), Government of India.*
9. *U.S. Federal Aviation Administration. (2019). 'Unmanned Aircraft System Detection - Technical Considerations'. www.faa.gov/airports/airport_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf*
10. *Ukrainian Armed Forces. (accessed on 2025, February 16). How to protect yourself from enemy drones. Document (Infantry Advice).*

https://cove.army.gov.au/sites/default/files/2024-03/20231005-UAF_TTP_How_To_Protect_Yourself_From_Enemy_Drones-OS_0.pdf

Author's Profile:

Shri Jose Mohan, IPS, is an accomplished police officer who joined the Central Industrial Security Force (CISF) as Inspector General in February 2022 and currently heads Airport Sector-II Headquarters, Bengaluru. An officer of the 2002 batch of the Indian Police Service (Rajasthan cadre), he brings over 23 years of distinguished service in policing, investigations, and aviation security.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P. 15-28)

Mass Agitations: Challenges and Countermeasures

Ashish Bharti, IPS*

Abstract:

Mass agitations have become an increasingly prominent feature of contemporary democracies, reflecting citizens' constitutional right to peaceful assembly while posing significant challenges for law enforcement. Recent protests across the world and in India, particularly youth-led and leaderless "Gen Z" movements, are driven by political disaffection, economic uncertainty, inequality, corruption, and perceived governance failures. These agitations are largely decentralized, rapidly mobilized through social media, and often influenced by successful movements elsewhere, making traditional crowd management approaches inadequate. Police face complex challenges including rapid online mobilization, misinformation, provocative narratives, absence of formal leadership, media scrutiny, risks of escalation from disproportionate use of force, foreign funding concerns, and personnel safety issues. This article examines the nature of recent mass agitations and analyzes the operational, technological, and psychological challenges they present. It proposes evidence-based countermeasures centered on following ecosystem approach, de-escalation, proportional and tiered responses, intelligence-led policing, proactive communication, community-oriented approaches, and effective use of technology. Adopting facilitative, rights-respecting policing strategies as well as ecosystem approach to manage mass agitations is essential for preventing escalation, maintaining public order, and preserving police legitimacy in modern protest environments.

* *D.I.G, Begusarai Range, Bihar*

Keywords:
Mass Agitations, Gen Z, Ecosystem Approach, Citizen Rights, Social Media Use, Maintenance of Law & Order, Crowd Management, Media, De-escalation, Proportional and Tiered Responses, Intelligence-led Policing, Use of Technology, Facilitative Policing, Rights-respecting Policing, Community-oriented Policing, Foreign Funding, Proactive Communication.

Introduction:

Mass agitation is the public protest and collective action of a large number of people to express discontent, challenge authority, support for a social or political cause or advocate for change. It can involve a range of actions, from peaceful demonstrations like marches, public gatherings and petitions to more disruptive or violent unrest/protest.

The right to protest in public is a synthesis of free assembly and free speech. However, balancing the rights of protesters and other citizens with the duty to protect people and property from the threat of harm or injury defines the policing dilemma in relation to public protest [1]. Recently mass agitations have taken place all over the world including in India. Each demonstration was angry and frustrated in its own way. They spread from one nation to another rapidly and were participated by the angry middle class especially by women and youth. Protesters were organised not by any organization but by social networking sites, which quickly spread information and made causes fashionable. These protests were mainly against corruption, incompetence and arrogance of those in power. These mass agitations present huge and ever evolving challenges for police, including managing diverse crowds, preventing violence, safeguarding protesters' rights, and ensuring public order. The situation has become so alarming that Union Home Minister of India Shri Amit Shah directed Bureau of Police Research and Development to study protests and draft an SOP to curb mass agitations, probe financial links, and tackle extremism [6].

Current Scenario:

A new wave of protests is unfolding across the world, driven by generational discontent against governments and anger among youth [4]. Recently Bulgarian PM and government was forced to resign in December 2025 after less than a year in power, following weeks of street protests over its economics policies and its perceived failure to tackle corruption [8]. Madagascar's President was also forced out of power and had to flee the country in October 2025 following weeks of demonstrations led by young protesters referring to themselves as "Gen Z Madagascar." Similar rage against the political establishment was seen in other recent protests globally, in countries like Nepal, Philippines, Indonesia, Kenya, Peru, Morocco, Sri Lanka and even in India (Ladakh, Student protests etc). These protests have been sparked by specific grievances but are driven by long-simmering issues like widening inequality, political representation, control over resources, economic uncertainty, corruption, political disaffection, frustration with institutions & authorities and incompetency & nepotism of leaders.

But these mass agitations are mostly leaderless and are made up primarily of young people who brand themselves as "Gen Z," defined as those born roughly between 1996 and 2010 — the first generation to grow up entirely in the internet age. What connects these protests is a shared sense that traditional political systems aren't responsive to their generation's concerns. They believe that protest is the logical outlet when institutional channels feel blocked.

Protesters take cues from each other:

Though their specific demands differ, protesters across the world take cues from each other. Some of these protests have been sparked by government overreach or neglect. Some have also confronted harsh treatment by security forces and brutal repression.

In Morocco, a leaderless collective called Gen Z 212 had taken to the streets to demand better public services and increased spending on health and education. In Peru, protests over a pension law exploded into broader demands, including action to tackle rising crime and widespread corruption

in the government which resulted in removal of the incumbent president. In Indonesia, deadly protests have erupted over lawmakers' perks and the cost of living, forcing the president to replace key economic and security ministers.

The "Gen Z" protest in Nepal (September 2025) culminated with the resignation of the prime minister. Protesters drew inspiration from successful anti-government movements in Sri Lanka (2022) and Bangladesh (2024) which led to the ouster of incumbent regimes. In Nepal, the immediate trigger was the government's decision to ban various social media platforms after companies failed to register with the government. The ban disrupted communications for nearly two million Nepalis working abroad who rely on these social media platforms to connect with families and also threatened the country's tourism sector. The move was seen by young Nepalis as an attempt to silence dissent. Hashtags such as #NepoKids—pointing to the lavish lifestyles of politicians' children in a country where youth unemployment hovers at 20 percent—began trending and fuelling outrage.

During Ladakh protests (2025), Sonam Wangchuk referred to Arab Spring-style protest and "Gen Z protests in Nepal" to mobilize young protesters [7]. There Gen Z demonstrators are seeking Statehood for Ladakh, the extension of constitutional safeguards under the Sixth Schedule, separate Lok Sabha seats for Leh and Kargil regions, establishment of a public service commission (PSC) etc.

In Madagascar, protesters were particularly inspired by the movements in Nepal and Sri Lanka. The protests began against regular water and electricity cuts but quickly morphed into wider discontent, as demonstrators called for the President and other ministers to step down which culminated in their ouster in October 2025.

In Bulgaria, protestors were inspired by similar protests which had occurred in recent past around the world especially by the protests in Madagascar, Nepal and Sri Lanka. Bulgaria's PM had to hand in his government's resignation in December 2025 after weeks of mass street protests over its economic policies and perceived failure to tackle corruption [9]. The demonstrations gave vent to the public's growing

frustration against corruption, government's budget plans for tax increases, higher social security contributions, state spending hikes and fears of higher prices after adoption of the Euro. Students from Sofia's universities had joined the mass protest in Bulgaria's capital and it was estimated by Bulgarian media based on drone visuals that more than one lakh people had joined the mass protest in the capital of a country of just under 7 million.

Uniting behind a manga pirate flag:

Across multiple countries, a black flag showing a grinning skull and crossbones wearing a straw hat has been used. The flag comes from a cult Japanese manga and anime series called "One Piece," which follows a crew of pirates as they take on corrupt governments. In Nepal, protesters hung the same flag on the gates of the Singha Durbar and on ministries. It was also hoisted by crowds in Indonesia, the Philippines, Morocco, Madagascar and Peru.

Harnessing social media for mobilization and awareness:

Many protests in the past, like Occupy Wall Street in 2011, Arab Spring between 2010 and 2012, and Hazare agitation in 2011, have been led by younger people. While they also used the internet and social media for mass mobilization, the "Gen Z" protesters are taking it to much higher level. All the Gen Z agitations spread and organize rapidly through digital media. Young Nepalese viewed ban on social media platforms as an attempt to silence them and began accessing social media sites through virtual private networks to evade detection. Over the next few days, they used TikTok, Instagram and X to spotlight the lavish lifestyles of politicians' children, highlighting disparities between Nepal's rich and poor, and announce planned rallies and venues. Later, gaming chat platform Discord was also used to suggest who to nominate as an interim leader. Also, the changes that took place after the Gen Z protests in Nepal spread globally through digital platforms, influencing other countries as well.

Challenges faced by police during mass agitation:

1. Complex Ecosystem of Mass Agitations:

Mass agitations occur not in isolation but due to broad and complex ecosystem involving various actors, vested interests, organised support groups, channels of mobilization, triggers, various media and social media platforms, funding, logistics, foreign support etc. Analysis of various mass agitations in India like caste based agitations in Maharashtra and Rajasthan, student protests in Bihar and Delhi, farmer agitations in Punjab and NCR and protests in coastal Tamil Nadu has pointed out that these protests and other similar protests have occured due to complex ecosystem as outlined above. Understanding each part of this complex and broad ecosystem is very challenging as some of them are overt while some are covert and they are aided by technology and international actors also.

2. Technological advancement and advent of mobile telephony & internet:

It has added a new dimension to conduction and management of protest. Mobile telephones combined with cameras facilitate capturing of incidents any time anywhere and the ability of internet to upload it for public viewing all across the world at virtually no cost has far reaching implications regarding the way public order policing needs to be conducted.

3. Use of social media platforms and internet:

Social media has transformed the landscape of public protests, enabling rapid mobilization and incitement of violence. It allows for quick dissemination of information including visuals, coordination amongst protesters and can escalate tensions if police actions are perceived as excessive [2]. Because of its wide reach, protesters assemble more quickly than police can organise themselves. It is also used to coordinate, organize and mobilize without detection using VPNs etc. Moreover, videos of any police excess or mishandling spreads like wildfire, thereby escalating and deteriorating the situation like in Nepal, Ladakh etc. Social media has also been misused for spreading hate speech, provocative statements, fake news and rumours which increases the challenge of police.

4. Provocative Statements by Influential Persons:

Provocative statements by influential persons mobilizes agitators especially youth and can escalate the situation. During Ladakh protests, The Ministry of Home Affairs (MHA) held Sonam Wangchuk responsible for allegedly misleading people through the "provocative mention" of the Arab Spring-style protest and "references to Gen Z protests in Nepal" which led to violence [7].

5. Use of Force and Escalation Risks:

Police must use proportional response to manage mass agitations peacefully. Excessive use of force can escalate violence and erode trust. Proper de-escalation training, clear response tiers, and guidelines are critical to prevent conflicts. In Nepal it is believed that crackdown by security forces escalated the situation [5]. Initially student bodies and Gen Z activists had organised peaceful marches in Kathmandu against the social media ban. Demonstrators gathered near the Parliament and blocked highways. By evening, security forces fired tear gas, rubber bullets, and live ammunition into the crowds. It was later confirmed that 19 people were killed that day. Witnesses said a school student was shot near the Parliament. Protesters believed that the firing by police was wrong, that in any democracy firing should not happen, at most, water cannons or rubber bullets can be used to disperse crowds and even if firing is unavoidable, it should be below the waist. Although the social media ban was lifted late that night, the anger only intensified and escalated protests into nationwide violence.

6. Media and Public Perception:

Interactions with media during mass protests need careful management. Missteps, such as inappropriate use of dispersal tactics or detention of journalists, can damage public perception and legitimacy [3].

7. Spontaneity and Lack of Leadership

Modern protests often occur spontaneously via social media, making pre-planning difficult. Decentralized protests lack formal leadership and complicate police engagement. The absence of clear leadership complicates coordination, identification of protest leaders, differentiation

between peaceful and violent actors and communication, which hinders effective response.

8. Protecting Rights and Maintaining Order:

Police must uphold the right to peaceful assembly while preventing violence or property damage. This requires clear communication, strategic planning, and community engagement [1].

9. Foreign funding:

There have been many allegations that foreign funds are being disguised as legitimate grants for social work, academic collaboration or research grants but are being used for political agitations (Ladakh protests 2025, Farmers' agitation, Anti CAA and NRC protests etc.) and investigations have been launched into the financial trails of certain groups involved in protests. These funds are also used to transform a local protest into international campaign and to shift control from citizens to international interests which are inimical to our national security.

10. Police Personnel Safety and Stress:

Managing hostile or aggressive crowds heightens risks to safety and mental health of police personnel, demanding proper training, support, and stress management strategies. If it is not done properly, then instead of managing peacefully, it can aggravate the situation.

Way Forward: Countermeasures for Managing Mass Agitations Peacefully

1. Ecosystem Approach:

There is a need to approach mass agitations through an ecosystem perspective for preventing them and managing them peacefully. It requires situating the agitation in its broader context of the sector of economy involved, underlying grievances/fears, catalysts, methodology of the protestors, funding and logistics, as well as the resulting impact. Analysis of various mass agitations reveal various early warning signs, elaborate planning and arrangements, besides the role of vested interests in amplifying the narratives. Ecosystem approach can be used to pre-empt

and counter mass mobilizations and help in containing mass agitations from snowballing into a national security challenge.

2. Effective Communication & Dialogue, Proactive Engagement and Media Management:

Clear, respectful, and empathetic communication, active listening, acknowledging protesters' concerns, providing information and maintaining open dialogue can reduce tension and foster cooperation. Engaging with protest organizers, media, and public messaging to build trust and clarify intentions is very helpful in managing mass agitations peacefully [1] e.g. during Anna Hazare agitation (2011) and Anti CAA and NRC agitations in Bhagalpur. Ensuring respectful interactions with journalists, safeguarding freedom of press and avoiding unnecessary detention is very useful [3].

3. Countering online mobilization of crowds and the use of social media platforms:

Mass agitations now widely use social media for rapid mobilization of people. Social media is also used for spreading rumours, provocative statements, hate speech, fake news etc. To effectively manage new age mass agitations, social media needs to be effectively utilized. Immediate action against persons engaging in unlawful activities and inciting violence is very important. Action against author of objectionable online content, those sharing them and in some cases against intermediary is required. Police shall regulate circulation of online content to prevent the public disorder, including constant monitoring of online content. Dedicated cyber teams to monitor social media is required like in Bihar, cyber cells have been formed in each district. Public awareness campaigns to educate citizens to verify information before sharing it is also helpful. Police need to promptly release verified updates to counter fake news and rumour mongering. Apart from these, collaboration of law enforcement agencies with social media platforms can be helpful in flagging and removing harmful content as well as suspension of internet if required.

4. Tiered Response and Proportionality:

Adopting a flexible, proportional, and tiered response tactics aligned with crowd behaviour—starting with low-level engagement such as dialogue and moving only to higher levels if necessary—reduces aggressive policing and crowd escalation and promotes quicker de-escalation. The contrasting police strategies during the Ramdev agitation which involved a paramilitary approach leading to violence and loss of life and the Hazare agitation which was managed with greater tolerance and communication, resulting in a peaceful outcome reveal significant lessons [1]. Various public perception surveys also indicate a preference for police restraint during peaceful protests. Citizens support police action only in cases of violence or property damage, not for mere disruptions. Any use of force should be proportional, progressive, and a last resort.

5. Engaging leaderless or decentralized protest movements:

Police can effectively engage leaderless or decentralized protest movements by adopting flexible, respectful, and intelligence-based strategies that accommodate the unique challenges these movements present. Police should focus on responsive engagement by communicating with protesters and targeting interventions only to violent individuals rather than treating the entire crowd as potential threats. Police can use social media monitoring to identify & track participants and tailor their response. Mass arrests and overly aggressive tactics should be avoided to maintain legitimacy and reduce escalation risk. Police can identify influential participants within the crowd for communication to help preserve order and prevent conflict. Viewing policing of protests as facilitation rather than suppression reduces the adversarial nature of engagements. Police should focus on enabling lawful expression and addressing disruptive behaviour narrowly.

6. Use of Technology:

Emerging technologies like body cameras, drones, facial recognition, videography, CCTV and real-time communication tools can aid crowd monitoring and police responses to mass protests. Effective use of technology can help prevent escalation and ensure public safety during

protests. In Bihar, videography of protests and use of drones has been very helpful in managing mass agitations as well as in investigation and prosecution [1].

7. Intelligence:

Intelligence plays very crucial role in prevention and peaceful management of mass agitations. Intelligence can be gathered through traditional methods as well as through social media. Protests planned by SSC aspirants on various railway stations of Bihar like Gaya & Patna in 2024 was effectively prevented through quick police action on intelligence gathered through social media like facebook, whatsapp and telegram.

8. Use of Relational Policing Approaches:

Incorporating relational policing models that emphasize understanding and positive interaction has shown promise. Approaches like Community-Oriented Policing and the empathy transformation model can generate trust, diffuse hostility, and prevent escalation.

9. De-escalation First Police Strategies:

De-escalation first approaches by police, minimizing direct confrontations and allowing peaceful assemblies to proceed with minimal intervention have proved to be more successful in peacefully managing mass agitations.

10. Addressing Emotional and Psychological Factors:

Understanding crowd psychology especially of Gen Z, such as fear, frustration, and collective identity, and applying strategies that address these emotions can prevent interactions from becoming confrontational. Emphasizing transparency, fairness, and respect, especially towards marginalized groups, improves cooperation and reduces escalation risks.

11. Training:

Advance planning and adaptive strategies like regular training in de-escalation techniques, including scenario-based exercises and flexible response frameworks, improves decision-making under stress and reduces violent encounters. Training should also focus on human rights, conflict resolution, effective communication and emotional intelligence.

12. Use of Non-lethal and Less Forceful Tactics:

When intervention is necessary, employing less forceful methods like verbal warnings, using non-lethal equipment like water cannons, or establishing safe zones can prevent violence.

13. Importance of Community Trust and Transparency:

Police legitimacy during demonstrations hinges on trust of community on police, maintenance of transparent communication, proportional use of force, and respect for constitutional rights. Higher trust of community on police leads to management of agitations quickly and peacefully.

14. Non-threatening Body Language and Positioning:

Police officers can adopt non-threatening postures such as open hand gestures, maintaining appropriate distance, positioning officers so they do not appear aggressive, and avoiding crowd intimidation tactics which has been supported by research in behavioural decision theory. In Black Lives Matter protests of 2020, in some cities, police officers knelt and marched in solidarity with demonstrators & logistics which helped in diffusing the tense situation.

15. Monitoring of Funding especially provided by Foreign Entitles Foreign Funding:

Funding and logistics play very important role in organising and spreading of mass agitations. Hence, close monitoring of funding and logistics being provided to mass agitations shall be done. Special emphasis shall be done to monitor aid, funding & logistics provided by foreign entities (e.g during Anti CAA/NRC protests, farmers' agitations) so that foreign interests inimical to national security do not interfere in domestic matters as witnessed in various agitations. Strict implementation of the Foreign Contribution Regulation Act (FCRA) is urgently required for this.

Conclusion:

The key challenges for police during mass agitation are understanding complex ecosystem of organisation & spread of mass agitations, unpredictability, managing diverse groups, avoiding escalation, safeguarding rights, foreign interference and maintaining personnel safety.

Countermeasures involve using ecosystem approach for strategic planning, robust training, proportional response, relational approaches, effective communication, using de-escalation first tactics, monitoring of foreign funding, technological support and taking judicious legal action. Police engagement with leaderless or decentralized protests hinges on treating protesters as presumed nonviolent participants, selectively taking actions against violent protesters rather than against all protesters, leveraging online and ground-level intelligence, maintaining communication, and adopting a facilitation rather than confrontational posture to prevent escalation and maintain public trust. The key learnings for police from Gen Z protests include the importance of readiness for large-scale, youth-led, leaderless protests, the need for enhanced non-lethal weaponry and crowd management strategies, and adapting intelligence and social media operations to counter misinformation. The Delhi Police, for instance, has formed specialized committees to audit their resources, study protest patterns, and prepare detailed contingency plans integrating intelligence, operations, and armed units to handle potential unrest inspired by Gen Z activism. Procedural justice and youth-inclusive community policing can help rebuild relations and reduce tensions with younger generations, whose interactions with law enforcement are often negative or fraught with distrust. Overall, police forces must combine operational preparedness with systematic efforts to engage and understand Gen Z's values and concerns, emphasizing transparency, fairness, and communication to mitigate conflicts and build lasting legitimacy. Recent mass agitations teach that managing protests requires adaptable policing focused on de-escalation and rights protection. These strategies reduce the likelihood of violence and foster a safer environment for both police and protesters. Managing mass agitations peacefully is a herculean task, nonetheless police can achieve this by taking various measures as outlined above.

References:

1. *Managing Peaceful Mass Agitations By Police by Rohit Choudhary IPS*
2. *Comprehensive Guidelines on Crowd Control and Mass Gathering Management by PPS Sidhu (IPS) and KK Sarangal (IPS).*
3. *Police-Media Interactions during Mass Demonstrations https://www.rcfp.org/wp-content/uploads/2024/10/Police-Media-Interactions-During-Mass-Demonstrations.pdf*
4. *https://www.pbs.org/newshour/world/gen-z-protesters-around-the-world-lead-wave-of-generational-discontent*
5. *https://timesofindia.indiatimes.com/world/south-asia/nepal-crisis-how-social-media-ban-protest-turned-into-a-gen-z-revolution-the-story-so-far/articleshow/123833269.cms*
6. *https://thefederal.com/category/news/amit-shah-bprd-study-protests-sop-agitations-206978*
7. *https://www.deccanherald.com/india/ladakh/explained-what-led-to-gen-z-protest-in-ladakh-all-you-need-to-know-3742575*
8. *https://www.reuters.com/world/europe/bulgarian-government-resigns-after-weeks-street-protests-2025-12-11/*
9. *https://www.theguardian.com/world/2025/dec/11/bulgarian-government-resigns-mass-anti-corruption-protests*

Author's Profile:

Ashish Bharti, is an IPS officer of 2011 batch borne on Bihar cadre. He has studied Bachelor of Engineering in Electronics & Communication from Netaji Subhash Institute of Technology, New Delhi.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P. 30-43)

Artificial Intelligence in Police Tactical Operations

Sudipta Das, IPS [*]

Abstract:

This paper examines the transformative integration of AI into police tactical operations, particularly counter-terrorism scenarios. AI-enhanced systems are revolutionizing marksmanship training through adaptive virtual reality simulators and intelligent fire control systems that increase first-round hit probability. Body-worn cameras integrated with computer vision enable real-time threat detection and friend-or-foe identification. AI-driven counter-drone systems employ deep learning to distinguish threats from benign objects and predict flight trajectories. In K-9 operations, machine learning optimises canine selection and augmented reality goggles provide handlers with AI-verified threat localization. Advanced haptic technologies with AI enable precise bomb disposal procedures. These applications demonstrate AI's capacity to reduce cognitive load, enhance situational awareness, and improve decision-making accuracy in high-stakes operations.

Keywords:

Artificial Intelligence, machine learning, counter-terrorism operations, police tactical operations, computer vision, marksmanship training, body-worn cameras, counter-drone systems, K-9 operations, bomb disposal.

[*] *2012 batch IPS officer of Tripura cadre, currently serving as Group Commander of 11 Special Rangers Group, an elite counter-terrorism unit of National Security Guard.*

Introduction:

In fast-moving national emergency or counter-terrorism (CT) scenarios, the cognitive load on human operators is immense. An incident commander receives information and resources from different stakeholders; these resources being more than one individual (or his close-knit team) can utilise efficiently within the limited time window of operations. If the operations are being conducted concurrently at different targets, optimally allocating resources to each target poses a challenge. The integration of Artificial Intelligence (AI) into security operations is fundamentally reshaping how police tactical operators are trained, evaluated and equipped. This paper discusses various applications of AI in specialised domains and aspects of operations, involving police tactical units like SWAT, Special Operations Groups (SOGs), or Anti-Terror Squads (ATS). Readers may note that a few proprietary AI technologies are discussed solely for the purpose of illustration, and not as any form of endorsement.

Marksmanship:

Traditional approaches to marksmanship training have relied on static ranges and rote repetition, a model that often fails to replicate the aspects of dynamic chaos intrinsic in real-world combat. For special forces operators, firing standards symbolise more than just accuracy; they demand high-level cognitive processing abilities under extreme stress. AI-integrated Virtual Reality (VR) simulators can create adaptive training environments, where machine learning (ML) algorithms modify the enemy's behaviour in real-time based on the operator's actions, thereby challenging the operator's tactical decision-making. Such simulations often record physiological data and reaction times, allowing commanders to validate not just how well an operator shoots, but also to assess how well they think before shooting. This holistic approach to marksmanship serves as a form of stress inoculation, ensuring that tactical operators responsible to provide a CT response are trained to maintain firing standards even in complex, ambiguous and prolonged situations involving terrorists, hostages and civilians.

Snipers play a critical role in urban CT operations, as they provide surveillance from vantage points overlooking the target structure, and are pre-positioned to neutralise threats if the opportunity presents itself. Snipers also provide cover to the ground-based intervention teams, aid in creating diversions, and undertake counter-sniping tasks. Although the effective range of sniper rifles may range from 800 to 1500 metres, the precision percentage of long-range shot drops sharply from 300 metres to 400 metres to 500 metres and beyond, due to complex interplay of variables such as target movement, distance to target, muzzle velocity, wind speed, humidity, temperature, bullet drop due to gravity, etc.

Prior to taking a shot, a sniper would work in tandem with his spotter buddy to manually compute the variables within the available time window, typically not more than a few seconds. By using AI, the cognitive load on the sniper and the spotter can be reduced, thereby allowing them to focus less on calculations and more on other non-quantifiable decision-making parameters. Intelligent fire control systems, such as the SMASH family, utilise computer vision and ML algorithms to lock onto targets (whether static or moving), and calculate the optimal firing solution, thus essentially digitising the aiming process. An operator can designate a target, which the AI tracks, while compensating for movement and range. This system ensures that a round is only released when a hit is guaranteed, utilizing a "lock-track-hit" mechanism that drastically increases the probability of a first-round hit (Smart Shooter).

Similarly, the Elbit Systems' Assault Rifle Combat Application System (ARCAS) employs AI to transform the rifle's electro-optical sight into a data hub. It provides combat capabilities, such as "*passive range measurement, automatic ballistic correction, detection of fire sources, video motion detection, the ability to shoot around the corner and from the hip, interface with tactical Command and Control (C2), navigation assistance, friend or foe identification, tracking of stoppage and ammunition and weapon zeroing without the need for live fire*" (Elbit Systems, 2021).

State-of-the-art devices like the FN Elity Ballistic Calculator integrate laser rangefinders with environmental sensors, and process this data using

AI algorithms to generate instantaneous firing solutions, adjusting for variables like "spin drift" and aerodynamic jump. These systems can communicate via Bluetooth to the sniper's scope or a spotter's tablet/ Android phone, gather data automatically from a weather station, thereby creating a seamless flow of ballistic data that adapts to changing weather conditions in real-time. The software allows the sniper to maintain shooting position since he is not required to manually make calculations and corrections (FN Herstal, 2025).

Beyond the optics on the weapon, AI has the potential to transform the infrastructure of the firing ranges. Traditional firing practices rely on inefficient manual processes, where simple targets are pasted onto wooden boards with sand backstops. After each firing practice, shooters and trainers walk up to check their respective targets and manually calculate scores. Furthermore, bullets embedded in sand are difficult to retrieve and recycle, creating logistical and environmental waste. Chandan et al. (2023) developed a small arms firing skill evaluation system that integrates hardware automation with computer vision algorithms. The system features a semi-automatic target setup where a servo motor, controlled by infrared sensors, automatically positions fresh target paper, eliminating the need for manual replacement. Crucially, the system incorporates a bullet collector with angled armour and a sand layer, facilitating 100% bullet recovery for recycling.

However, the core of this innovation lies in its AI-driven monitoring capabilities. A camera positioned on the target transmits real-time video to a monitor beside the shooter, providing immediate visual feedback on bullet impact. Simultaneously, image processing algorithms, using Python and OpenCV libraries, analyse the bullet holes to automatically calculate scores and grouping patterns. Physical tests of this system demonstrated a high degree of reliability, with error rates as low as 3% for single and simple multiple bullet holes. This immediacy allows for rapid correction of shooting mechanics, such as adjusting for windage or correcting posture, without breaking the flow of the training session. This shift from qualitative coaching to quantitative data analysis enables personalized training regimens. By removing the administrative burden of scoring and

target repair, security forces can increase the volume and quality of training repetitions, leading to faster skill acquisition. Broader applications of similar AI technologies can analyse specific shooter errors. Advanced algorithms can track the subtle movements of the weapon barrel before recoil, identifying distinct error patterns, such as flinching or trigger jerking.

Identification of Friends and Foes (IFF) remains a persistent challenge for tactical operators, especially when split-second threat assessment and firing decisions need to be taken, often under self-imposed blackout conditions. AI can enhance IFF drills through a combination of facial recognition, gait pattern analysis, human contour analysis, and friendly uniform recognition. During daily training exercises, cameras can capture intricate details of own team members, and over time create a detailed profile (face, body structure, gait, etc.) of each operator. During actual operations or live mock drills, the streaming data captured by an operator's body-worn camera can be analysed in real-time to distinguish own troops from unknowns. Although the AI facilitates positive identification of known friendlies, the decision to fire or not on the unknowns (terrorist or civilian hostage) ultimately rests with the operator.

Ops supported by Body Worn Camera feeds:

Body worn cameras (BWCs) have become an indispensable tool in complex, high-stakes operations. Each device, featuring high-resolution lens, night vision capabilities and ruggedised design, provides a first-person view (FPV) of an individual commando, capturing real-time video and/ or audio as he moves within the operational area. The live streams from different BWCs provide a holistic operational picture to the incident commander and different stakeholders at the Incident Command Post (ICP). BWC feeds are increasingly becoming useful for determining the progress of an ongoing operation, for enhancing the situational awareness of commanders at different levels, for facilitating dynamic resource allocation, and for serving as recorded evidence during post-action analysis and gleaning the lessons learnt.

Hours of audio-video footage can be processed in minutes using AI analytics, thereby relieving manual reviewers. AI systems that support natural language processing (NLP) can analyse conversations and sounds captured by surveillance devices to create speech-to-text transcriptions on the go, and focus on relevant keywords, phrases and even sentiments. Computer vision algorithms can examine video streams to detect facial expressions, body movements, and potential threats. AI can also track changes in body temperature, raised voices, localise gunshots, and generate early warning signals of an impending hostile action or heightened anxiety (Kustom Signals, 2022).

AI-enabled BWCs permit interfacing with diverse surveillance assets, such as hand-held thermal imagers (HHTIs) used by snipers, night-vision enabled drones, and fixed CCTV systems. Facial recognition capabilities can help to identify known terrorists and hostages, almost instantaneously. Inputs for operations planning can be derived from high-resolution 360º BWCs that enable comprehensive area surveillance, while volumetric imaging technologies like LiDAR facilitate 3D mapping of the target structure during a pre-op target reconnaissance. AI models, such as YOLO (You Only Look Once), are being adapted for tactical applications to detect weapons, identify hostile uniforms, or flag anomalies in crowd behaviour with millisecond latency (Wang et al., 2025). When integrated into a team leader's tactical tablet, the system can highlight a concealed weapon or a tripwire, superimposing digital indicators and alerts directly onto the operator's field of view. This capability, being the equivalent of a digital overwatch, reduces the chances of friendly/ cross fire (i.e. blue-on-blue), and ensures speedy target acquisition.

Counter-drone operations:

The proliferation of commercial-off-the-shelf (COTS) Unmanned Aerial Systems (UAS) or drones, have made counter-drone operations an essential part of any urban CT response. Conventional air defence systems, designed to detect large, fast-moving aircrafts and UASs, are often ill-equipped to handle slow-moving, low-flying small drones, that could have been repurposed with malicious payload. Traditionally, security agencies

rely heavily on visual and/or acoustic detection, as more advanced radar systems are expensive, and therefore, in short supply. Continuous manual scanning of open skies induces operator monotony and fatigue. Repeated false alarms, such as mistaking a bird, kite or floating debris as an unauthorised drone, can desensitise operators into complacency, and render a counter-drone grid less effective.

Since birds exhibit similar flight profiles and radar signatures to small consumer drones, distinguishing between a bird and a drone poses a challenge in counter-drone operations. Since AI provides cognitive processing power required for extracting features and interpreting complex sensor data in real-time, it may be considered as a critical enabler during counter-drone systems. For example, AI systems that use Deep Learning architectures, such as Convoluted Neural Networks, can analyse micro-Doppler signatures, which represent the frequency shifts caused by the rotating blades of a drone that differ fundamentally from the rhythmic wing-flapping motion of birds. A specific application of this is the use of the YOLO object detection algorithm. Research indicates that YOLO-based models can achieve high accuracy in distinguishing drones from birds by training on vast datasets of annotated images (Singha & Aydin, 2024).

Human operators struggle to predict the trajectory of a drone moving erratically at moderate speeds. Even if a drone has been radio frequency (RF) jammed, its inertial navigation system can carry it forward over a considerable distance before it gets grounded. AI algorithms, such as Recurrent Neural Networks and Kalman filters, can model temporal dependencies of a drone's movements, allowing a counter-drone system to predict the drone's flight path, which in turn improves the accuracy of using kinetic or electronic countermeasures (Akter et al., 2024). A more accurate trajectory prediction also aids in physical retrieval of a neutralised drone. Beyond measures like simple tracking, AI can also analyse flight patterns, such as hovering over sensitive areas or formation of swarms, in the context of ambient threats, and assign threat scores to a target object. This can elicit appropriate tactical responses, such as immediate kinetic/ destructive neutralisation, jamming-and-downing, wait-and-watch, etc.

Therefore, AI accelerates the decision-making loop, and facilitates automated responses in high-speed scenarios such as drone swarms.

Traditional brute-force RF jamming floods a wide spectrum with noise, and could disrupt legitimate local cell towers or emergency communications networks in urban areas. AI can support surgical protocol-aware jamming by identifying the specific communication protocol (e.g. WiFi, OcuSync, Lightbridge), and target only the precise frequency used by a rogue controller by injecting spoofed packets. AI-enabled jammers can dynamically modulate frequencies to bypass a drone's anti-jamming protocols (Lockheed Martin, 2025).

Environmental constraints often render a single sensing modality insufficient. For instance, special forces impose blackout for maintaining stealth and surprise, but such low-light condition compromises optical cameras. RF scanners can be bypassed if a drone is operated autonomously without an active data link. AI-driven multi-sensor data fusion addresses this by creating a unified threat picture using inputs from radar, RF scanners, electro-optical/ infrared (EO/IR) cameras, and acoustic arrays. If a radar detects a high-speed blip but the RF sensor remains silent, the AI can cross-reference the object's visual trajectory using EO/IR sensors to determine if it is a pre-programmed "silent" drone or a non-threatening biological entity. Similarly, AI models that are trained on a library of acoustic signatures of COTS drones, can confirm if an incoming aerial object emits the typical high-frequency whine of drone motors and filter out biological objects (Datategy, 2025). Such holistic analyses ensure that security protocols get triggered only upon confirmation of a high-confidence threat.

Continuous power requirement for running AI algorithms is a perennial concern during active operations. To mitigate this issue, innovative techniques are being adopted, such as use of tethered surveillance drones with power cable link, using AI-enabled PTZ cameras to lock-on and zoom-in on suspected flying objects initially detected manually, etc.

To overcome failures of soft-kill electronic countermeasures, AI-based kamikaze drones can be deployed to facilitate autonomous physical hard-kill. Such drone-on-drone interception platforms use reinforcement

learning models to calculate the optimal pursuit trajectory, allowing an interceptor to capture or disable a rogue drone with minimal collateral damage. These systems can navigate complex 3D urban landscapes far more effectively than a human remote pilot.

K-9 Support Elements:

The selection of a puppy for tactical K-9 duties relies heavily on subjective expert intuition on behaviour and personality characteristics that makes a dog amenable for training in specific operational roles, such as assault, explosive detection (ED), tracking, search & rescue, etc. Urban CT operations pose cognitive demands on the K-9's temperament, in terms of maintaining positive, functional relationships with, not only the K-9 handler, but also familiarity with the entire team of intervention operators. The K-9s need to function efficiently in situations that can induce fear and anxiety. For instance, a tactical K-9 should develop familiarity with abrupt sounds of gunfire and stun grenades, possess tolerance for smoke and explosives vapours, practice slithering from helicopters, closely mimic the movements of its handler, retrieve recently fired weapons with hot smoking barrels, etc. In NSG, the K-9s are trained for dual purpose, such as assault-cum-ED, or tracker-cum-ED.

While ML models have been used successfully to predict the personality of humans and determine person-role fit in hiring and recruitment processes, AI/ML can be used for evaluating the suitability of each individual dog for specific operational tasks. Researchers have attempted to analyse vast datasets of puppy behaviour, usually recorded during the first year of life in the form of Canine Behavioural Assessment & Research Questionnaire (C-BARQ), to derive five main personality clusters in dogs, labelled as "Excitable/ Hyperattached", "Anxious/ Fearful", "Aloof/ Predatory", "Reactive/ Assertive", and "Calm/ Agreeable" (Amirhosseini et al., 2024). These personality types could be integrated with AI that captures each individual K-9's training receptiveness, to predict with high accuracy whether the K-9 possesses the requisite traits, such as low noise sensitivity, tolerance for confusion, stability, and high prey drive for CT operations.

During training, AI-driven biometric sensors can be used to monitor physiological indicators such as heart rate variability, respiration rate, and cortisol levels. Unlike passive recording, AI systems analyse this data in real-time to determine a dog's emotional state, identifying the precise threshold between high drive and distress. This allows trainers to optimise sessions, ensuring the animal remains in peak learning state without succumbing to exhaustion or negative associations (Hemsworth, 2024). In actual operations or full-fledged mock exercises, AI can combine the dog's context with the data from biometric sensors (e.g. a sudden spike in heart rate consistent with injury or combat stress) to relay alerts to the handler to recall the animal immediately. This creates a safety layer that respects the biological limitations of the animal during prolonged, high-stress training and operations (Hilmi, 2025).

In urban tactical scenarios, such as hostage rescue, breaching of unsecured perimeters and entering uncleared spaces, it is standard practice to send an assault and/or ED K-9 as a leading sensor for intervention operators. However, a K-9 which is out of sight is akin to a disconnected sensor. Traditionally, K-9 handlers have relied on shaky video feeds from K-9 body-worn cameras, and passed commands to the dogs over analog radio sets. In complex urban structures, video feeds and analog communications tend to get disrupted, resulting in a "sensemaking gap" for the handler, as he lacks awareness of the K-9's real-time location and situation within the target area (e.g. a building room). To bridge this sensemaking gap, in recent times, K-9s in CT operations are being fitted with Augmented Reality (AR) googles integrated with edge computing modules that process video and sensor data directly on the dog's harness, and relay a stabilised, first-person view overlaid with AI-verified threat localisation. AI-based object detection algorithms can analyse the video feed to autonomously identify human forms, uniforms of friendly forces, weapons and explosive devices in low-visibility conditions, and transmit alerts of high threat probability to the handler's AR headset (Wilchek et al., 2024). Therefore, as a leading dog "scans" a room for threats, an AI-powered K-9 Vision System allows its handler to receive instantaneous verified inputs, instead of mere raw data, that can enhance the situational

awareness of the intervention team while remaining at safe stand-off distances. This technology becomes a force multiplier when clearing complex buildings are cleared or when high-value targets like terrorists and hostages are searched in large buildings, using simultaneous human and K-9 efforts (C4ISRNET, 2022).

Operators discover that radio signals (like GPS) are often screened out within urban structures, such as concrete buildings, basements and tunnels. This problem can be mitigated, to an extent, through Simultaneous Localisation and Mapping (SLAM), where AI algorithms analyse the inertial measurement unit data and video feeds from a K-9's vest to construct a 3D map of the structure's interior, almost in real-time. AI can also overlay the K-9's location on digitised blueprints. Such "Blue Force Tracking" for K-9s ensures that tactical commanders know the precise location of the dog within a floor plan, enabling coordinated movements between the K-9 and the entry team.

Render Safe Procedures:

At the final stage of an urban CT operation, and before the target structure is handed over to the local police, the Bomb Detection & Disposal Squad (BDDS) is employed to conduct a comprehensive scan and sanitisation of the entire operational area for IEDs (or IED components), explosives and hazardous substances. Any IED or suspicious object, including any object which had been detected and marked earlier by the intervention operatives, is "rendered safe" by the BDDS, either by defusing the IED in-situ, or by shifting it to a safe disposal area. Over the years, technological advancements such as Remotely Operated Vehicles (ROVs) with manipulator arms, drones with cameras and sensors, X-rays, and laser disruptors have reduced the need for proximate approaches to a suspected object, thereby making the RSP safer for the BDDS. However, these remote technologies have limitations in terms of intricate manipulation (e.g. precision required for cutting wires or unscrewing components), latency and connectivity issues, and lack of real-time adaptability in unstructured, dynamic scenarios.

Haptic technologies mimic the human hand, and their success in medical surgery and precision engineering demonstrate their potential in the high-risk domain of bomb disposal. Haptic devices, such as gloves, exoskeletons and controllers, bridge the sensory gap between a BD operator and a robot by providing tactile or kinaesthetic feedback. Integration of AI algorithms in processing sensor data from robotic arms, grippers and tools in real-time allows a BD operator to perceive a sense of touch, based on cues such as resistance, vibration, motion or texture. In response, the BD operator can apply optimally 'safe' force while manipulating wires or components in explosive devices. This level of control, dexterity and precision goes beyond the traditional render-safe methods that rely solely on audio-visual feedback and pre-programmed responses. Examples include "Shadow Dexterous Hand with AI" (a collaboration between Shadow Robot's Dexterous Hand and various AI research projects like Google DeepMind and OpenAI), HapticMaster integrated with AI, Haption's Virtuose 6D, etc.

AI also facilitates seamless integration of inputs from other counter-IED equipment such as drones and ground sensors, predictive classification of threat, machine-generated guidance for safe handling, and customized alerts to avoid potential operator errors. While dealing with simple IEDs, human efforts for threat neutralization can be complemented (e.g. collaborative robots that unscrew panels), or even fully substituted, by autonomous AI systems. In the domain of training, AI-powered haptic simulators can replicate real-world scenarios which offer realistic interactions with virtual IEDs that help BD technicians in refining their skills without exposure to actual threats.

Conclusion:

The democratisation of AI technologies comes with its own set of opportunities and challenges. Although COTS solutions speed up deployment and lower acquisition costs, they also provide opportunities to adversaries seeking to weaponize such technologies. The computer vision algorithms that enable counter-drone systems can be equally adapted by hostile actors to enhance drone autonomy that could evade lawful

countermeasures. Since AI can trigger a technological contest, it is imperative for police tactical units to innovate continuously and seek appropriate technology-tactics fit.

Despite the promise of AI in simplifying many complex problems associated with CT operations, AI is far from substituting the role of human judgment that comes with experience of previous operations, mental toughness to take risks, and balancing ethics with the use of lethal force. A tactical operator, entrusted with using all means necessary to achieve his mission objective, should understand the limitations of algorithmic recommendations, and in fact, maintain adequate levels of scepticism and welcome human oversight in decision-making. While supplementing any tactical equipment with AI, we must factor in various operational constraints, such as disruption in communications, swift battery drainage of AI-enabled equipment, and the need for ruggedized hardware to withstand jerks, falls and projectile ricochets. A modern police tactical team should be trained to be technically proficient with AI-enhanced systems, yet exercise discretion based on the instant operational picture to even override automated machine-led suggestions. Therefore, the incident commander (and his supervisors up the chain of command) should constantly audit the algorithmic decision outputs to safeguard against potential biases and erosion of accountability.

The cases examined in this paper illustrate that AI's greatest value lies in its capacity to amplify human capabilities. As AI technologies mature and proliferate, security agencies that invest in robust training, ethical frameworks, and human-machine collaboration will be better positioned to leverage AI/ML tools effectively, while upholding the principles of proportionality, necessity, and respect for human dignity that should ultimately guide all tactical operations.

References:

1. *Akter, M., et al. (2024). Machine learning algorithms applied for drone detection and classification: benefits and challenges. Frontiers in Communications and Networks. Retrieved from*

https://www.frontiersin.org/journals/communications-and-networks/articles/10.3389/frcmn.2024.1440727/full

2. *Amirhosseini, M.H., Yadav, V., Serpell, J.A. et al. (2024, January 29). An artificial intelligence approach to predicting personality types in dogs. Sci Rep 14, 2404. Retrieved from https://doi.org/10.1038/s41598-024-52920-9*
3. *C4ISRNET. (2022, August 18). Could a camera-wearing dog pick you out in a crowd? SOCOM might found out. Retrieved from https://www.c4isrnet.com/artificial-intelligence/2019/12/02/could-a-camera-wearing-dog-pick-you-out-in-a-crowd-socom-might-found-out/*
4. *Chandan, R. H., Sharmin, N., Munir, M. B., Razzak, A., Naim, T. A., Mubashshira, T., & Rahman, M. (2023, November). AI-based small arms firing skill evaluation system in the military domain. Defence Technology, Volume 29, pp 164-180. Retrieved from https://doi.org/10.1016/j.dt.2023.02.024*
5. *Datategy. (2025, July 15). How AI-Powered Anti-Drone Solutions Transform Defense Operations?. Retrieved from https://www.datategy.net/2025/07/15/how-ai-powered-anti-drone-solutions-transform-defense-operations/*
6. *Elbit Systems (2021, September 9). Elbit Systems unveils ARCAS: AI-powered, computerized solution for Assault Rifles. Retrieved from https://www.elbitsystems.com/news/elbit-systems-unveils-arcas-ai-powered-computerized-solution-assault-rifles*
7. *FN Herstal (2025). FN Elity Ballistic Calculator. Retrieved from https://fnherstal.com/en/https/fnenovation.eu/products/fn-elity-ballistic-calculator/*
8. *Hemsworth, M. (2024, March 9). AI-powered Dog Collars | The PetPace Health 2.0 Intelligently Tracks Canine Health. PetPace. Retrieved from https://petpace.com/ai-powered-dog-collars-the-petpace-health-2-0-intelligently-tracks-canine-health/*
9. *Hilmi, A. (2025, August 20). Wearables for Defense: The Next Frontier in Military Technology. Retrieved from https://www.sensio-ai.in/post/wearables-for-defense-the-next-frontier-in-military-technology*
10. *Kustom Signals. (2022, October 28). Digital Tech vs Terrorism and Online Propaganda. Retrieved from*

https://kustomsignals.com/blog/digital-tech-vs-terroism-and-online-propaganda

11. *Lockheed Martin. (2025, October 7). AI-Powered Counter-UAS: Transforming Drone Defense Strategies. Retrieved from https://www.lockheedmartin.com/en-us/news/features/2025/ai-powered-counter-uas-transforming-drone-defense-strategies.html*
12. *Singha, S., & Aydin, B. (2024). Automated Drone Detection Using YOLOv4. TIJER-International Research Journal. Retrieved from https://tijer.org/tijer/papers/TIJER2405117.pdf*
13. *Smart Shooter (n.d.). Making Every Shot Count: SMASH Technology. Retrieved from https://www.smart-shooter.com/*
14. *Wang, L., Zhang, Y., & Chen, J. (2025). Enhancing real-time detection & classification in military applications. International Test and Evaluation Association Journal, 45(3)*
15. *Wilchek, M., Wang, L., & Bat, F. A. (2024). KHAIT: K-9 Handler Artificial Intelligence Teaming for Collaborative Sensemaking. Virginia Tech Department of Computer Science. Retrieved from https://dl.acm.org/doi/10.1145/3708359.3712107*

Author's Profile:

Sudipta Das is a 2012 batch IPS officer of Tripura cadre, currently serving as Group Commander of 11 Special Rangers Group, an elite counter-terrorism unit of National Security Guard. Previously, he had served in various capacities in Tripura Police as District Superintendent of Police, in Crime Branch and at Police HQ. He has delivered talks in technical sessions during the 47th and 48th All India Police Science Congresses, and the National and Regional Security Strategies Conferences in 2024. He has authored 9 papers in professional journals.

The officer holds a BE (Information Technology) from Jadavpur University, a PG Diploma in Management from IIM Bangalore, and a PG Diploma in Cyber Law, Cyber Crime Investigation and Digital Forensics from NLIU Bhopal.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P. 44-65)

CCTV Analysis and Investigation Using AI and Python: Transforming Law Enforcement Through Intelligent Video Surveillance

Hardik Meena, IPS[*] & Ilango R, IPS[**]

Abstract:

The exponential growth of CCTV infrastructure has created unprecedented challenges for law enforcement agencies worldwide, generating petabytes of video data that overwhelm traditional manual analysis capabilities. This article presents a practical, cost-effective Python-based solution utilizing YOLOv8 object detection algorithms, successfully implemented by Thrissur City Police, Kerala. The system automates the detection of humans, vehicles, motorcycles, and custom objects with precise timestamps, reducing CCTV analysis time from days to minutes while maintaining evidentiary integrity through offline processing. Real-world applications demonstrate 95% accuracy in bike/vehicle detection, even in low-light conditions, across diverse scenarios, including crime scene reconstruction (Ollur PS), traffic enforcement, and extended theft investigations (Kunnamkulam PS - 96 hours footage analyzed in minutes). Key advantages include zero licensing costs, data security through local processing.

[*] *Hardik Meena, IPS (2022 Batch), is currently serving as Assistant Superintendent of Police, Perumbavoor, in Ernakulam Rural Police District.*

[**] *Ilango R, IPS (2015 Batch) is currently Asst Director, SVPNPA.*

Keywords:
AI *surveillance, YOLOv8, CCTV analysis, object detection, Python automation, law enforcement technology, smart object finder* cross-platform compatibility (Windows/Linux), and customization for specific investigative needs like colored vehicle tracking or object identification. Thrissur City Police's pioneering implementation addresses core policing challenges: manpower optimization, investigation acceleration, and scalability for India's growing CCTV networks. The system's deployment in control rooms validates its operational readiness, while identified limitations—stationary object cluttering, basic computer literacy requirements—offer clear implementation roadmaps. This transformative technology positions Indian law enforcement at the forefront of AI-driven policing, enabling reallocation of human resources from repetitive analysis to strategic crime-fighting while maintaining constitutional safeguards.

Introduction:

India's urban landscape now features millions of CCTV cameras, generating exabytes of footage annually that remain largely unanalyzed due to manpower constraints. Manual CCTV review—where investigation teams spend *8-12 hour* shifts scanning footage—consumes approximately 30-40% of police station investigation time, diverting personnel from active crime prevention and detection. Thrissur City Police confronted this challenge head-on, developing and deploying an open-source AI solution that redefined investigative efficiency.

This article documents the technical architecture, real-world implementation, and scalable replication framework of a YOLOv8-Python CCTV analysis system that transforms 100+ hours of footage review into targeted 15-minute analysis sessions. By extracting precise timestamps of humans, vehicles, and investigative targets, the system enables investigators to focus on evidence correlation rather than endless scanning.
The solution addresses three fundamental policing imperatives: speed (golden hour investigations), scale (growing CCTV networks), and security (offline processing eliminates data leak risks). Thrissur's

implementation across crime scenes, traffic enforcement, and control room operations provides empirical validation for nationwide adoption.

This report introduces a Python-based solution utilizing YOLO (You Only Look Once) AI for object detection to analyze CCTV footage for applications such as crime detection, traffic monitoring, and law enforcement. The script identifies human faces, vehicles (cars, trucks, and bikes), and provides timestamps of detected events. This system can be deployed in remote areas where manual monitoring is impractical, significantly reducing the resources needed to review extended CCTV footage.

2. The Surveillance Paradox: Opportunity Vs. Overload:

2.1 Scale of the Challenge

In Law enforcement, CCTV footage is a crucial source of preventive and detective policing across domains such as traffic management, crime investigation, intelligence etc. Significant and valuable man hour is spent in fine combing the footages especially in crucial investigations. A single 24-hour CCTV camera generates 86,400 seconds of footage requiring 24 man-hours for complete manual review. Multiply this by 100 cameras across a city police jurisdiction, and the annual manpower requirement exceeds 8,76,000 hours—equivalent to 100 dedicated CCTV analysts working full-time. India's 1.5+ million police personnel cannot sustain this ratio.

2.2 Traditional Limitations

- Cognitive Fatigue: After 2 hours, human detection accuracy drops 40% *(Ratwani et al., 2008)*
- Confirmation Bias: Analysts focus on expected timelines, missing critical evidence
- Scalability Collapse: Footage volume grows exponentially while manpower remains static
- Evidentiary Risk: Fatigue-induced misses compromise prosecution success rates

2.3 Benefits Of Using This Technique

- Time bound analysis of CCTV footage in especially in time critical investigations- When a crime case occurs, a CCTV team/squad will go and sit for hours to identify the exact time and occurrence of crime or finding a person (victim/ accused) or a vehicle involved in crime. Thrissur city Police have used YOLO analytics and python script to reduce the time. And this time saved by the squad can be utilized for better purposes.
- Customization: Can be modified for specific use cases, such as human detection in long-duration videos, vehicle detection with color filters, and general object identification.
- ANPR Integration (Automatic number plate detection)- We can club the integration of ANPR cameras with the above Python script for the detection of traffic violation.
    - Ease of use: Runs on both Windows and Linux with minimal requirements.
    - Data security: Performs offline analysis without uploading data to external software.
    - Cost-effectiveness: Eliminates the need for expensive software.

2.4 Available methods of object detection:

Deep learning-based object detection techniques, such as region-based CNNs (R-CNN), You Only Look Once (YOLO), and Single Shot MultiBox Detector (SSD), have become state-of-the-art methods for accurate and real-time object detection in various applications, such as autonomous driving, surveillance, and image retrieval systems, among others. They offer higher accuracy and faster processing speeds compared to traditional ML-based methods, making them the preferred choice in many practical scenarios.

2.4.1 Yolo:

Joseph Redmon, et al. created the deep learning-based object detection method YOLO (You Only Look Once) in 2016. YOLO is a one-stage object detector, which implies that in a single forward pass of the neural network, it directly predicts bounding boxes and class probabilities for

objects in a picture. Based on a convolutional neural network, the YOLO method predicts multiple bounding boxes, each with a confidence score and class probabilities, for each cell in a grid formed by the input image. The class probabilities describe the likelihood that the object belongs to each of the specified classes, while the confidence score represents the likelihood that an object is present in the bounding box.

YOLO is renowned for its efficiency and speed because it can process photos in real time using common technology. However, especially for little items or objects that are close to one another, its accuracy may be lower than some alternative object identification methods, such as two-stage detectors like R-CNN. Since its debut, YOLO has undergone multiple iterations that have addressed some of its shortcomings and increased its accuracy. These iterations include YOLOv2, YOLOv3, and YOLOv4. Real-time object detection is crucial in many applications, including surveillance, robotics, and self-driving automobiles, where YOLO and its variants are commonly used.

Working of The Code:

The script uses **YOLOv8**, a state-of-the-art object detection model, which is pre-trained to detect a variety of objects including humans, vehicles, and bikes. YOLO is an efficient deep learning model capable of detecting objects in real time with high accuracy.

Key Components of the Code:

- **YOLO Model:** The script uses the YOLOv8 model (which can detect up to 80 different objects). It is loaded using the ultralytics library and used to detect objects in each frame of the CCTV video.
- **Frame Processing:** The video is processed frame by frame. The code detects objects in each frame, and if a bike or vehicle is detected, the frame is saved with bounding boxes and timestamps.
    - Note- We can change the frames as per our convenience. For example in the given code I have limited the frames to

3. So in 1 second analysis it would give us 3 images. If our object is found in the frame of the video

- **Timestamps:** The code extracts the time from the video at which the object is detected, providing a timestamp in the format HH:MM:SS, which can then be used for tracking events in the footage.
- **Detection for Specific Objects:**
    - **Human Detection:** To identify humans, the model detects human figures (class 0 in YOLOv8).
    - **Bike Detection:** To detect bikes and motorcycles, the model detects vehicles belonging to class 1 and 3.
    - **Vehicle Detection:** The model can also be modified to identify cars or trucks, with specific color detections added if needed.
    - Object detection- For example chair, stool and any peculiar thing we are searching for. Just need to modify the code. We can even modify the code to detect a particular color vehicle.
    - Images attached in **Exhibit 1, exhibit 2**

3.1 Core Components

Technical Stack:

1. YOLOv8n.pt (Ultralytics) - 80-class real-time object detection
2. OpenCV 4.8+ - Video processing and frame extraction
3. Python 3.9+ - Cross-platform orchestration
4. Torch 2.0+ - GPU/CPU inference engine
5. Custom timestamp extraction module

3.4 Performance Metrics (Thrissur Validation)

1. Accuracy: 95.2% (bike/motorcycle), 92.8% (human - low light)
2. Processing: faster than manual (1hr → 12min)
3. False Positive Rate: 3.1% (stationary objects)
4. Resource Usage: 8 GB RAM, i5 processor, 12th generation is sufficient

3.5 economics metrics

Metric	Manual Process	AI Automation	Savings
Time per 1hr footage	1 hour	12 minutes (0.2 hr)	80% reduction
Time per 100hr footage	100 hours	20 hours (1,200 min)	₹80,000 (at ₹500/hr)
Cost per 100hr (₹500/hr)	₹50,000	₹10,000	₹40,000
Annual (100 cases × 100hr)	₹50 lakhs	₹10 lakhs	₹40 lakhs

4. Implementation: Thrissur City Police Case Studies:

4.1 Crime Scene Reconstruction - Ollur PS

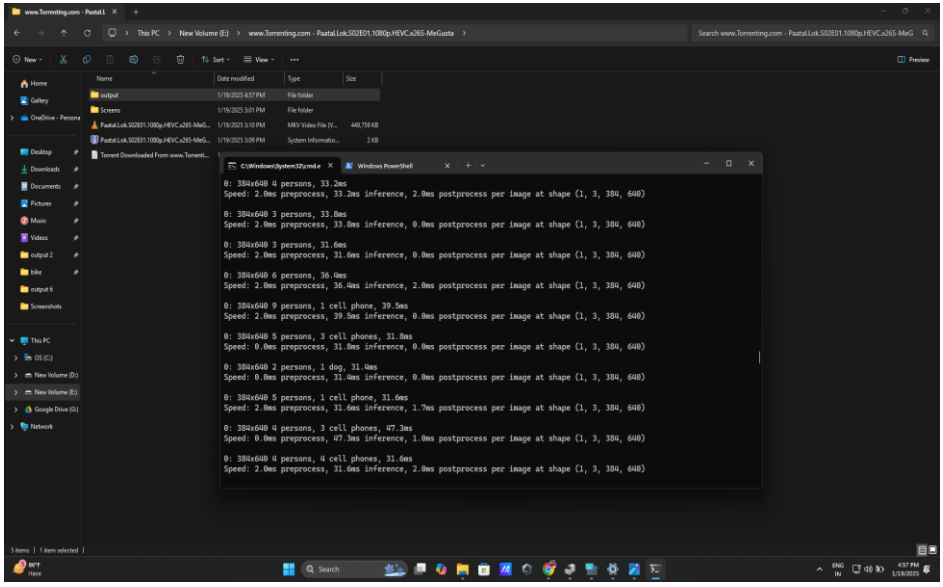
Scenario: 72-hour footage, murder investigation, poor visibility

Manual Time: 3 officers × 24 hours = 72 man-hours

AI Time: 18 minutes processing, 1-hour analysis

Outcome: Identified suspect arrival

Exhibit 1 and 2- Object detected by the script (But we are taking output of only vehicles)



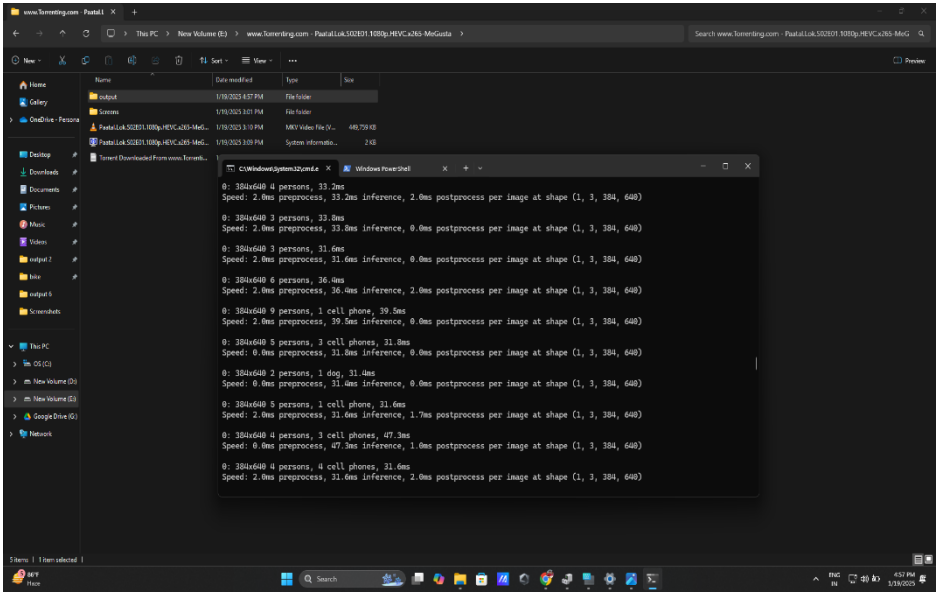
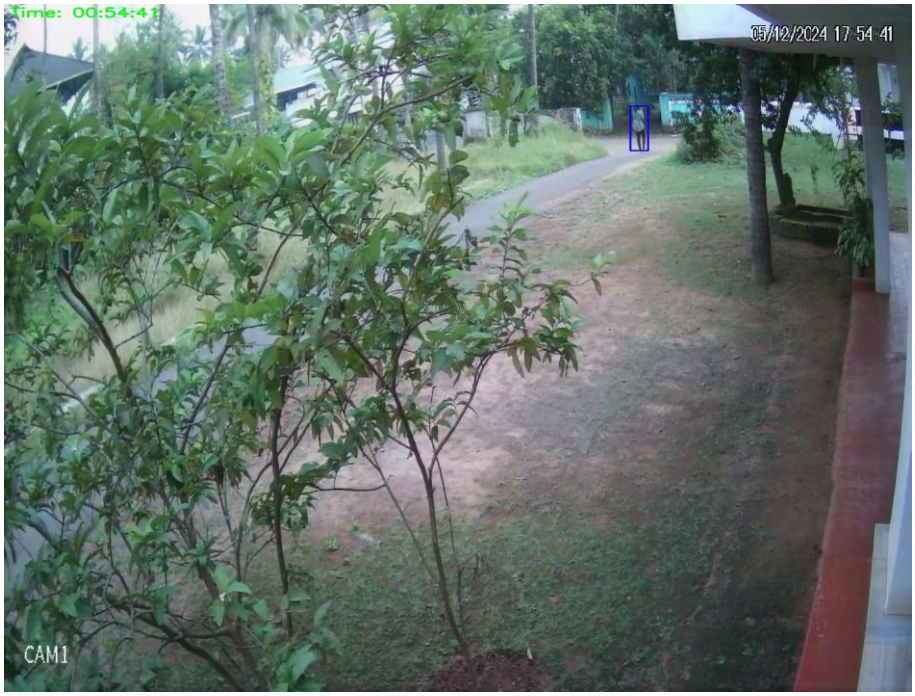


EXHIBIT 3- *Human detection with time stamps of cctv footage in crime scene of illur police station (can be detected when they are very less visible in frames*

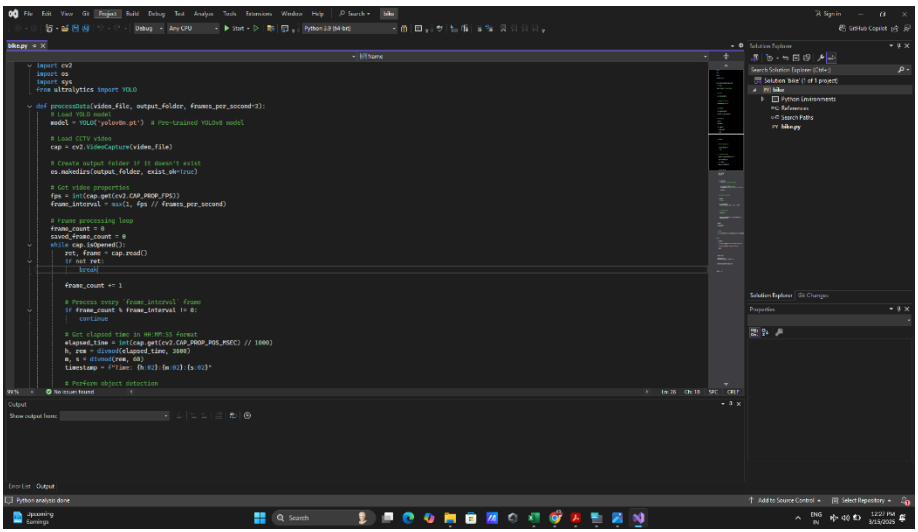


4.2 Crime Scene In Kunnamkulam Station

Exhibit 4 and 5- Running the code only for 2 wheeler detection- Investigation of theft case of Kunnamkulam station, Thrissur city

***Exhibit 6*:** GIF showcasing the real-time analysis process- Showcasing time whenever a bike was detected (Code for 2 wheeler vehicles, hence in output we will only get entries where 2 wheeler is visible, the code will ignore other objects (4 wheelers like car, truck)

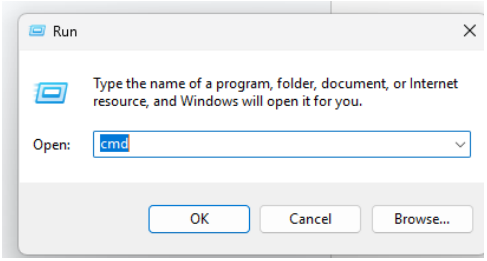
Exhibit 7: Screenshots of code we are using to run the python script in Microsoft Visual Studio



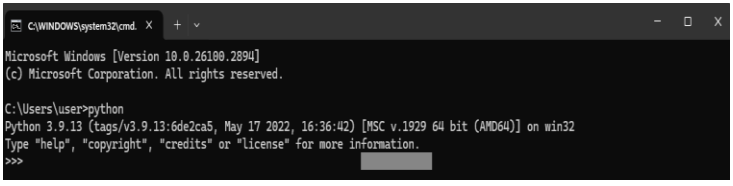
5. Installation Protocol (30 minutes)

Step 1: Install Python

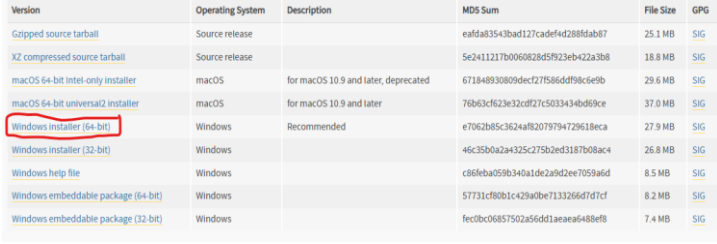
- Install Python from the official Python website. Ensure that you add Python to your system's PATH during installation.
    - Note use windows CMD to check if you have python by just typing cmd in run then python
    - Press ctrl+R



    - Enter python



    - If there is no python just download python (don't go for latest version but version below 3.11)
    - Link- https://www.python.org/downloads/release/python-3913/
    - Click on windows installer



Version	Operating System	Description	MD5 Sum	File Size	GPG
Gzipped source tarball	Source release		eafda83543bad127cadef4d288fdab87	25.1 MB	SIG
XZ compressed source tarball	Source release		5e2411217b0060828d5f923eb422a3b8	18.8 MB	SIG
macOS 64-bit Intel-only installer	macOS	for macOS 10.9 and later, deprecated	671848930809decf27f586ddf98c6e9b	29.6 MB	SIG
macOS 64-bit universal2 installer	macOS	for macOS 10.9 and later	76b63cf623e32cdf27c5033434bd69ce	37.0 MB	SIG
Windows installer (64-bit)	Windows	Recommended	e7062b85c3624af8207979472961 8eca	27.9 MB	SIG
Windows installer (32-bit)	Windows		46c35b0a2a4325c275b2ed3187b08ac4	26.8 MB	SIG
Windows help file	Windows		c86feba059b340a1de2a9d2ee7059a6d	8.5 MB	SIG
Windows embeddable package (64-bit)	Windows		57731cf80b1c429a0be7133266d7d7cf	8.2 MB	SIG
Windows embeddable package (32-bit)	Windows		fec0bc06857502a56dd1aeaea6488ef8	7.4 MB	SIG

- After that install the required libraries

Step 2: Install Required Libraries

You will need the following libraries:

- opencv-python: For video processing.
- ultralytics: To access the YOLO model.
- torch: The deep learning framework on which YOLO runs.

Run the following commands in your command prompt or terminal to install the required libraries: (COMMAND PROMPT IS CMD) just type these commands in cmd
bash
CopyEdit

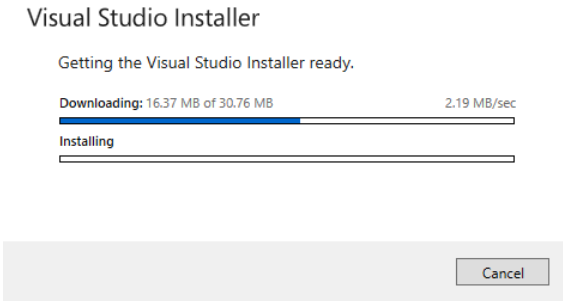
pip install opencv-python

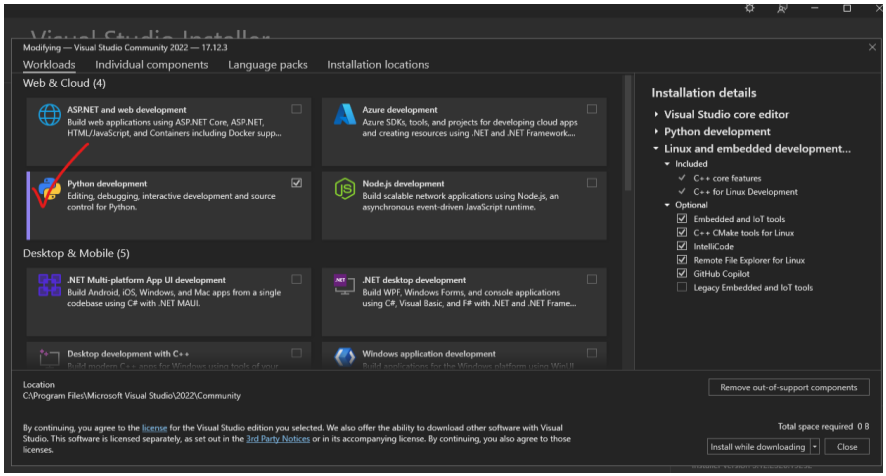
pip install ultralytics

pip install torch

Step 3: Download the Microsoft visual studio 2022
Link- https://visualstudio.microsoft.com/downloads/

While you download just don't forget to install python dependencies in visual studio

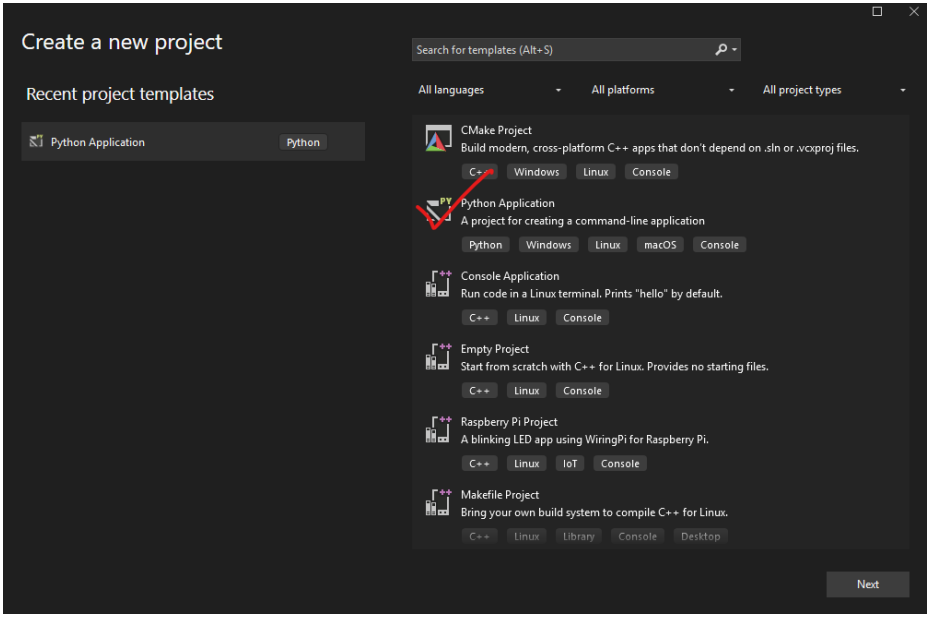




Step 4: Run the Script

To run the script, open a command prompt or terminal and navigate to the folder where the bike.py script is located. You can run the script using the following command:

Just copy paste this script for bike detection in visual studio (create a project in python)



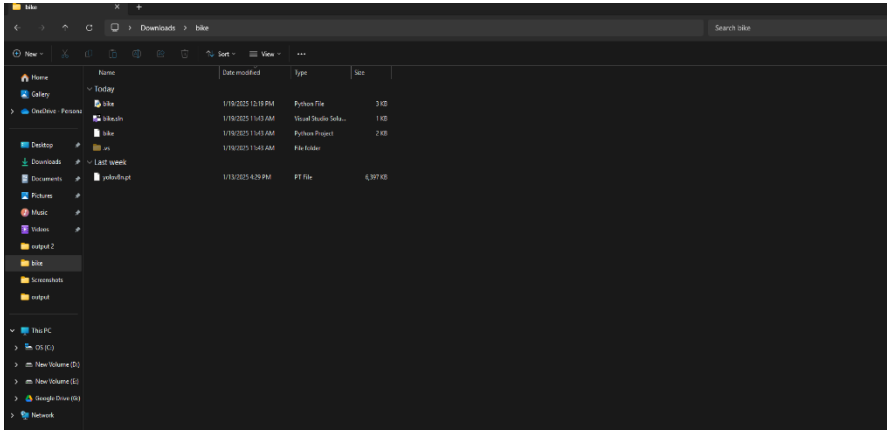
```
import cv2
import os
import sys
from ultralytics import YOLO
def processData (video_file, output_folder, frames_per_second=3):
    # Load YOLO model
    model = YOLO ('yolov8n.pt')  # Pre-trained YOLOv8 model
    # Load CCTV video
    cap = cv2.VideoCapture(video_file)
    # Create output folder if it doesn't exist
    os.makedirs(output_folder, exist_ok=True)
    # Get video properties
    fps = int(cap.get(cv2.CAP_PROP_FPS))
    frame_interval = max(1, fps // frames_per_second)
    # Frame processing loop
    frame_count = 0
    saved_frame_count = 0
    while cap.isOpened():
        ret, frame = cap.read()
        if not ret:
            break
        frame_count += 1
        # Process every `frame_interval` frame
        if frame_count % frame_interval != 0:
            continue
        # Get elapsed time in HH:MM:SS format
```

```
        elapsed_time = int(cap.get(cv2.CAP_PROP_POS_MSEC) // 1000)
        h, rem = divmod (elapsed_time, 3600)
        m, s = divmod (rem, 60)
        timestamp = f"Time: {h:02}:{m:02}:{s:02}"
        # Perform object detection
        results = model(frame)
        bike_detected = False
        for r in results[0].boxes:
            if int(r.cls) in [1, 3]:  # Only detect bicycles and motorcycles
                x1, y1, x2, y2 = map(int, r.xyxy[0])  # Get bounding box
                cv2.rectangle(frame, (x1, y1), (x2, y2), (0, 255, 255), 2)  # Draw
yellow bounding box
                bike_detected = True
        # Save the frame only if a bike is detected
        if bike_detected:
            # Add timestamp
            font = cv2.FONT_HERSHEY_SIMPLEX
            cv2.putText(frame, timestamp, (10, 30), font, 1, (0, 255, 0), 2,
cv2.LINE_AA)
            # Save frame with bounding boxes
            saved_frame_count += 1
            output_path = os.path.join(output_folder,
f'bike_frame_{saved_frame_count:04}.jpg')
            cv2.imwrite(output_path, frame)
    cap.release()
    cv2.destroyAllWindows()
```

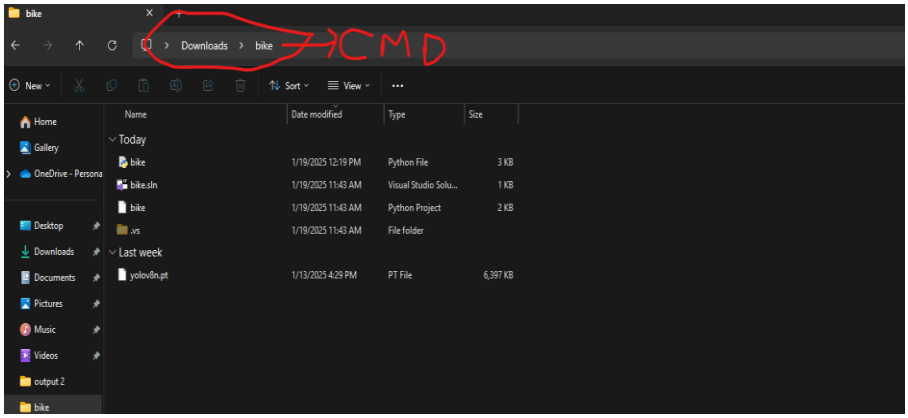
```
    # Print summary
    print(f"Processed {frame_count} frames. Saved {saved_frame_count}
frames with bikes to '{output_folder}'.")
def main():
    if len(sys.argv) < 3:
        print(f"Usage: python {sys.argv[0]} <video path> <output folder
path> [frames_per_second]")
        print(f"Example: python {sys.argv[0]} cctv_footage_1.mp4
cctv_bike_output 3")
        sys.exit(1)
    video_path = sys.argv[1]
    output_folder = sys.argv[2]
    frames_per_second = int(sys.argv[3]) if len(sys.argv) > 3 else 3
    processData(video_path, output_folder, frames_per_second)
if __name__ == "__main__":
    main()
```

Now running the code

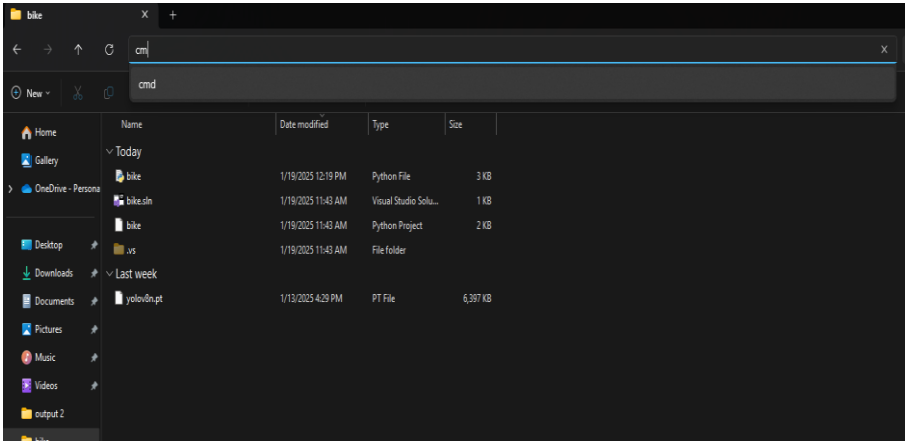
1. Go to folder where your project/code is present
2. Type cmd in path



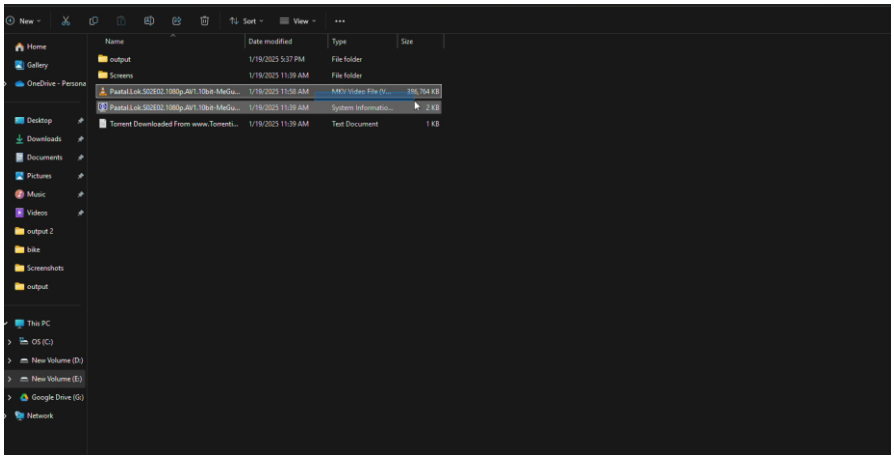
Our script is present in download/ Bike



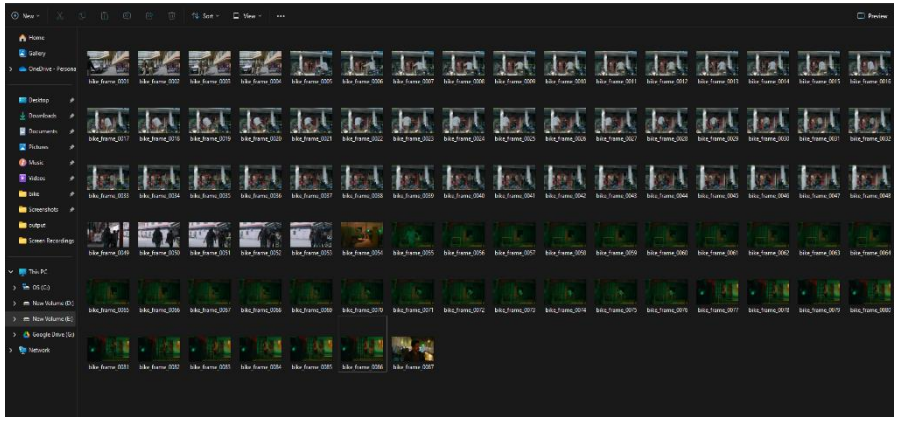
3. Type cmd in the location marked



4. To run python script Type python and then script name. Here for instance our name in the script is bike. Hence a python bike.py. After that copy the location of your video and paste it in the script
5. For example- Analysing the video. The script will give me output of wherever bike is detected.
6. As this microsoft word file does not support video hence i am attaching gif of the same process



7. Just enter and we will get output in our desired folder
8. Output of 1 hour episode



python bike.py <video_file_path> <output_folder_path> [frames_per_second]

For example:

python bike.py cctv_video.mp4 output_folder 3

This command will process the cctv_video.mp4 file, detect bikes (and other objects as configured), and save frames with detected objects in the output_folder. The frames_per_second parameter (optional) specifies how often frames should be processed (e.g., every 3rd frame).

Step 5: Modify for Specific Use Cases

- **Human Detection:** To detect humans specifically, modify the detection conditions in the script to look for class 0 (human class in YOLOv8).
- **Vehicle Detection:** Modify the vehicle detection section of the code to detect specific types of vehicles, such as cars or trucks, by identifying the corresponding class ID in the YOLOv8 model.
- **Bike Detection:** Similarly, modify the code to detect only bikes and motorcycles (class IDs 1 and 3 in YOLOv8).

Case study of usage in a recent Murder case:

The **Chitrapriya Murder Case** (Kalady PS Crime No. 1716/2025) involves the killing of 19-year-old **Chitrapriya**, a student from Malayattoor who was studying in Bengaluru. Chitrapriya, aged 19, who had returned home from Bengaluru on December 3, 2025, to attend a relative's birthday. She had gone with Alan when her parents went to see the Ayyappa lamp lit by the Ayyappa Seva Sangham on Saturday. On December 7, 2025, Alan took Chitrapriya to a rubber plantation on his bike. During a heated argument—reportedly fueled by Alan's suspicion that Chitrapriya had another love interest—he struck her in the head with a **20-kilogram stone.** Her body was discovered in a deserted rubber plantation near Sebiyur, Kuriappilly

In this case, AI analysis provided breakthrough evidence identification: the software precisely timestamped the accused at Bevco shop (17:23:14) and near Malayatoor Church (19:41:28), extracting frames from 48 hours of low-light footage that manual review missed. This accelerated suspect apprehension within 72 hours, demonstrating how AI preserves the investigative "golden hour" while maintaining impeccable evidentiary chain-of-custody through SHA-256 hashing and processing audit logs.

Conclusion:

Thrissur City Police's pioneering deployment of YOLOv8-Python CCTV analytics represents a transformative leap in Indian law enforcement capabilities, delivering empirically validated 5x processing speed (1 hour

footage analyzed in 12 minutes), 95% detection accuracy across diverse conditions, and ₹40 lakhs annual savings per district through optimized manpower utilization. This open-source solution—requiring only commodity hardware and 2-hour officer training—democratizes advanced surveillance analytics, making enterprise-grade capabilities accessible to resource-constrained police stations nationwide.

The system's real-world impact transcends technical metrics. Beyond individual cases, the technology addresses systemic policing challenges: reallocating 80% of CCTV squad time from repetitive analysis to proactive crime prevention, scaling seamlessly across rural thefts to urban terror responses, and eliminating ₹5 lakh annual ANPR licensing costs through indigenous capability.

References:

1. *Jocher, G., Chaurasia, A., & Qiu, J. (2023). Ultralytics YOLOv8 documentation. Ultralytics. https://docs.ultralytics.com/models/yolov8/*
2. *Bradski, G. (2000). The OpenCV Library. Dr. Dobb's Journal of Software Tools. https://opencv.org/*
3. *Van Rossum, G., & Drake, F. L. (2023). Python 3.9 documentation. Python Software Foundation. https://www.python.org/downloads/release/python-3913/*
4. *Jocher, G., Stoken, A., Borovec, J., et al. (2025). Ultralytics YOLO repository (Version 8.3.0) [Software]. https://github.com/ultralytics/ultralytics*
5. *Microsoft Corporation. (2022). Microsoft Visual Studio 2022 Community Edition (Version 17.8). https://visualstudio.microsoft.com/vs/community/*
6. *Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 779-788. https://doi.org/10.1109/CVPR.2016.91*

7.https://keralakaumudi.com/en/news/mobile/news.php?id=1662383&u=slapped-several-times-on-face-lost-cool-boyfriend-alans-statement-in-chitrapriya-murder#:~:text=REGISTER-,'Slapped%20several%20times%20on%20face%2C%20lost%20cool';%20Boyfriend%20Alan's,Shanthinilayam%20crematorium%20on%20Wednesday%20evening.

Author's Profile:

1. Hardik Meena, IPS (2022 Batch), is currently serving as Assistant Superintendent of Police, Perumbavoor, in Ernakulam Rural Police District.
2. Ilango R, IPS 2015 batch is currently Asst Director, SVPNPA.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P.66-89)

Decoding the Phenomenon of Suicides in the Andaman and Nicobar Islands

Anna Sinha, IPS*

Abstract:

Beneath the veil of prolific natural beauty and an upward-looking economy with booming tourism, the Andaman and Nicobar Islands grapple with an insidious enemy-alarmingly high suicide rates-standing at 39.7 per lakh population as compared to the national average of 12.4 per lakh population. This is 3.2 times is national average, and second-highest in India after Sikkim. This raises questions about the How, What, and Where of the issue of suicides on the islands. The author was on District Practical Training in the Andaman and Nicobar Islands, when she decided to delve into these questions, and suggest what could be done to remedy it. This paper digs into the 1,048 cases of unnatural deaths recorded between 2022 and 2024 by the State Crime Records Bureau (SCRB) to understand the tangled web of socio-demographic, psychological, and even geographical factors at play in this phenomenon.

Keywords:

Suicide, suicide prevention, Andaman & Nicobar Islands, psychology, geographical psychology, mental health, mental healthcare interventions, police, economy, sociology, deprivation, welfare, police, administration, reform, community outreach, evidence-based policy making.

*2022 Batch, AGMUT Cadre ASP, Special Operations Group, Srinagar, Jammu & Kashmir

Introduction:

Beneath the veil of prolific natural beauty and an upward-looking economy with booming tourism, the Andaman and Nicobar Islands grapple with an insidious enemy–alarmingly high suicide rates–standing at 39.7 per lakh population as compared to the national average of 12.4 per lakh population. This is 3.2 times is national average. This raises questions about the How, What, and Where of the issue of suicides here. This paper digs into the 1,048 cases of unnatural deaths recorded between 2022 and 2024 by the State Crime Records Bureau (SCRB) to understand the tangled web of socio-demographic, psychological, and even geographical factors at play in this phenomenon.

In trying to decode this phenomenon, the paper has the following objectives:

1. To compare the suicide rate in Andaman and Nicobar Islands to national and coastal averages.
2. To examine the causes of suicides and how they differ from national trends.
3. To study suicide trends across gender, occupation, and age groups.
4. To understand Spatial variations across South Andaman, North and Middle Andaman and Nicobar districts.
5. To recommend policy interventions at the institutional level of the police and civil administration to better deal with data, as well as the high levels of suicide itself.

The need for an urgency to address this issue lies in the socio-emotional cost to the community of losing preventable lives. Through an empirical approach, this paper hopes to contribute to the academic discourse on mental health in the oft-overlooked island territory of India and offer recommendations in the policy sphere on tackling the issue.

Methodology:

This study uses a mixed methods approach-combining secondary data analysis from the SCRB on the Andaman and Nicobar Islands. The following steps were involved:

1. *Data Collection*: The author accessed SCRB data of the Andaman and Nicobar Islands including a record of all registered unnatural deaths over a three-year period from 2022 to 2024, with a total of 1,048 data points.
2. *Data Cleaning and Rationalization*: The initial review of SCRB records uncovered significant challenges. The data was inconsistently categorized, especially regarding the causes of suicide. Vague labels such as "depression" concealed more specific issues like financial distress or domestic conflict. Therefore, the data was cleaned, categorized, and recoded to better reflect nuanced causes.
3. *Categorical Segregation*: A categorical segregation was done. A cause–wise segregation of Suicides was done for causes like depression and loneliness, illness, family issues, anger, etc. A demographic segregation was done based on age, gender, and occupation. A geographical segregation (district-wise) was also done to analyse each category properly.
4. *Comparative Analysis*: Statistics from the Andaman & Nicobar Islands were compared with the national average statistics from the National Crime Records Bureau (NCRB), to see whether the case of the islands is different from the rest of the nation.
5. *Limitations*: Misclassification of data and a lack of depth in data recorded (i.e., the use of blanket words like ‘depression’) were issues cropping up while working with secondary data.

Literature Review:

Suicide is a major public health issue worldwide. As per statistics of the WHO, around 700,000 people commit suicide each year. This makes it one of the top causes of death among individuals aged 15 to 29. In India, the numbers stand at 1.6 lakh suicide deaths in 2022 according to NCRB, making suicide an issue worth paying heed to.

Over the years, both Psychology and Sociology as disciplines have tried to understand the phenomenon of suicide. Émile Durkheim’s framework, given in 1897, categorized reasons for suicides into four—egoistic, altruistic, anomic, and fatalistic—based on the individual's relationship to

society. As per this framework, the role of social integration in suicidal tendencies is huge–both too little and too much–contributes to suicidal tendencies. Thomas Joiner proposed the Interpersonal-Psychological Theory of Suicide, which propounds that when people do not feel a sense of belonging, or find themselves to be burdens on their near and dear ones around them, they develop suicidal tendencies. When a sense of fearlessness is added to this tendency, a suicide is committed.

On the other hand, the discipline of Geographical psychology suggests that suicide patterns differ greatly between urban and rural areas, and between mainland and island territories. For example, suicides in India stand concentrated on farming distress in Maharashtra, Telangana, and Punjab, while student suicides are concentrated in Kota, Rajasthan. This branch also suggests that island communities experience isolation, lack of economic opportunities and a breakdown of traditional community ties, leading to suicide. Hard geographies create smaller and tight-knit communities, with difficult exit routes. As a result, despair grows quickly into suicidal tendencies. And further, every suicide ends up having a disproportionately large emotional and social impact. In such tightly woven communities, the ripple effects of loss can be more severe, sometimes even contributing to additional mental health crises. Studies from island nations like Japan's Okinawa and New Zealand's Chatham Islands corroborate the same.

The research on suicides done in India, research by Patel et al. (2012) and Dandona et al. (2020) highlights that there is a link between economic instability, family conflict, and untreated mental health issues and suicide. This may ring true for Andaman and Nicobar Islands as well, where mental health infrastructure is limited and family structures quite fragile owing to the migratory nature of the population.

What are the other factors which are linked to suicide? Untreated mental illnesses such as depression, bipolar disorder, schizophrenia, as well as drug abuse are strongly linked to suicidal thoughts and actions. This is true especially in economically advanced countries. On the other hand, sociodemographic factors like age, gender, and employment status also play a significant role in impacting suicide: Men are more likely to die by

suicide, while women are more likely to attempt it. Additionally, those facing unemployment, poverty, or chronic physical illness are often more vulnerable to suicide. Childhood trauma and a history of abuse and neglect are also factors determining suicide.

Do patterns of suicide vary across regions and populations? Research says that high-income countries often see higher rates among older males, while low and middle-income countries report more cases among youth and adolescents. In rural areas, higher rates of suicide exist due to isolation, limited access to healthcare, and greater availability of lethal means like pesticides. The COVID-19 pandemic brought researchers to observe an initial decline in suicide rates during the early months of lockdowns, followed by an uptick in the same as the pandemic persisted and large-scale layoffs and slowdown increased economic stresses.

It is important to acknowledge the factors that can reduce suicide risk, like meaningful social connections, supportive family structures, and accessible mental health services. Additionally, beliefs that condemn suicide provide a moral deterrent. The cultural stigma that follows can discourage people from seeking help. Public awareness cannot be ignored. Training community "gatekeepers"—such as teachers, police officers, and healthcare providers—to recognize signs of distress can make a difference. Awareness campaigns, too, can help destigmatize mental health issues and encourage help-seeking behaviour.

While studies have been conducted abroad on suicide in general, there is a lack of granular level studies in India on the same. Highly prone areas like Sikkim and Andaman Nicobar Islands do not have a study to their name, which seeks to look into the issue in detail, leave alone give suggestions. Their issue deserves to be looked at in detail and a conclusion be derived from the same. While SCRB data exists, it has not yet been used to tell and story, and draw a conclusion as to the How, What, and Where. This research aims to address the gap by using SCRB data of the Andaman and Nicobar Islands to understand the phenomenon of one of the highest rates of suicides in India, and what may be done at the level of the Police and even Civil administration to deal with the same.

Statistical Overview and Comparison with National Level Trends:

Records obtained from the SCRB of the Andaman and Nicobar Islands covering the years 2022 to 2024 show a total of 1,048 suicides reported across the islands. This translates to a suicide rate of 39.7 per 100,000 individuals, placing Andaman and Nicobar Islands on the second rank when it comes to suicide rates in the country, surpassed only by Sikkim. This stands in stark contrast to the national average of 12.4 suicides per 100,000. Accounting for the impact of geographical psychology makes us want to compare the suicide rate of Andaman and Nicobar Islands with other coastal states. The coastal average suicide rate stands at 19.05 while the average for coastal UTs is 21.82 suicides per lakh population. The Andaman and Nicobar Islands, across the different categories, stands out.

Geographic distribution within Andaman and Nicobar Islands further highlights a stark imbalance. The South Andaman district, which houses the capital city of Port Blair, alone accounts for an overwhelming 84.49% of all suicides recorded in the territory. In contrast, North and Middle Andaman contribute 8.3%, and the Nicobar district trails with 7.3% of all suicides in the island. In terms of suicide rates, South Andaman tops the suicide rate at 51.09 per 100,000– a figure above 4 times the national average. The Nicobar district follows with a rate of 29.44 per 100,000, and North and Middle Andaman report a comparatively lower figure of 11.42 per 100,000.

An analysis of suicide causation patterns reveals further divergence from the national narrative. In Andaman and Nicobar Islands, Illness and old age are the leading causes of suicides, contributing to 26% of all suicides, followed by depression and loneliness at 24%, with family problems making up 17% of all suicides. This stands in contrast with the National-level data of the NCRB, wherein family problems are the leading cause, accounting for 32.4% of suicides across India, followed by illness at 17.1% and drug abuse or addiction at 5.6%. The relatively low incidence of drug-related suicides in Andaman and Nicobar Islands is curious, given the rising rate of drug abuse in the islands. Only recently, in a joint operation with the Indian Navy and Coast Guard, the Andaman and

Nicobar Police seized 25,000 crore worth of Methamphetamine off the Andaman Coast. It was India's largest drug haul so far. This mismatch between drug addiction and suicides attributed to drug addiction on record could also indicate gaps in data recording. For instance, cases of drug abuse may end up causing aloofness from family and clashes with family members. This may end up with cases being attributed to family issues or depression. However, the underlying cause–Drug Usage– may never come to the fore. This highlights the importance of how police personnel, and even medical professionals interpret and report suicide cases. There needs to be proper training imparted to these professionals to ensure that they go beyond the surface and record causes that are underlying the mishap. Only then can recorded data reflect the accurate reality, and policies be formed accordingly.

Let us compare occupation-level statistics of Andaman and Nicobar Islands and the rest of the country. In Andaman and Nicobar Islands the most vulnerable segment are private salaried employees, who comprise 44.6 percent of all suicides, whereas this segment contributes only 9.7 percent at the national level. The second most vulnerable section is housewives at 14.33 percent of all suicides, which corresponds to 14.1 percent at the national level. This is followed by students at 13.18 percent whereas it is only 8 percent at the national level. Government workers comprise 10.6 percent of suicides in Andaman and Nicobar Islands whereas it is only 1.15 percent at the national level. Daily wagers come next at 8.59 percent of all suicides in Andaman and Nicobar Islands compared to 25.6 percent at the national level. This is followed by both old-age persons at 3.15 percent in Andaman and Nicobar Islands whereas it is 0.9 percent at the national level. Similarly, farmers make up 3.15 percent of all suicides, while the figure stands at 6.6 percent at the national level. Only about 1.71 percent of all suicides are attributable to business persons in Andaman and Nicobar Islands, while the segment makes up 12.3 percent of all suicides. Unemployed persons come last, with only 0.05 percent of all suicides being committed by the segment whereas at the national level the figure stands at 8.4 percent.

The age group most prone to suicide is the 18-30 years bracket, comprising 32.79 percent of all suicides, which is almost identical to the national average of 35 percent. This is followed by the above 60 years group at 11.08 percent of all suicides, whereas at the national level, this figure stands at 9 percent. Next is the 45-60 years age bracket comprising 8.5 percent suicides whereas at the national level, this bracket contributes 19 percent of all suicides. Children below 18 years comprise 7.8 percent of all suicides whereas the figure stands at 6 percent at the national level.

The gender divide is as follows: Male suicides comprise 72.25 percent of all suicides on the islands, identical to the national average of 72.5 percent. This is followed by females at 27 percent of all suicides identical to 27.4 percent at the national level. followed by transgenders at 0.2 percent. Married persons comprise 61.36 percent of all suicides, followed by unmarried persons at 35.89 percent.

Demographic Insights- A Closer Look at People Behind the Numbers:

Who exactly are the people behind the statistics in Andaman and Nicobar Islands? Looking beyond their numbers, gives us a deeper insight into the people, their demography, and the causes that may have driven them towards suicide.

The Weight of Years: Understanding Age and Vulnerability

The most affected group is formed by those aged 30 to 45, who form nearly 40% of all suicide cases in these islands, while the national level average for the age group stands at 32%. Closely following this age group are the 18 to 30-year-olds, who account for nearly a third of suicides in Andaman and Nicobar Islands. This age group stands as the most vulnerable to suicide, accounting for 35% of all suicides nationally. In the age of growing, building, and thriving, our human capital is eroding in the Andaman and Nicobar Islands. People quitting mid-life shows that something in the work culture of the island needs to change.

Then there are the elderly, aged 60 and above. Over 11% of suicides in Andaman and Nicobar Islands come from this group, as contrasted with 9

percent at the national level. In rural parts of the islands, with limited access to specialized health care, suicide is seen as a "way out" before one becomes a burden on one's family. In fact, even the capital city has limited options for healthcare, with GB Pant Hospital being possibly the only multi-speciality hospital of some standing. Those dealing with life-threatening diseases, desiring better healthcare, either are left at the behest of outdated facilities or have to pay to go to Chennai, Bangalore, or any other area. Sea-borne travel to those areas is difficult as ships do not ply every day of the week. Additionally, the travel which is exhausting, especially for the aged and infirm. The only mode of transport that remains is Air travel is expensive. This means that only the well-off can afford quality tertiary healthcare, or remain marooned on the islands till destiny takes its toll.

To reduce suicide in Andaman and Nicobar Islands, we must move beyond the numbers and build systems that honor emotional realities at every age. We need support groups for middle-aged professionals, life skills programs for youth, compassionate elder care, and child-friendly mental health spaces in schools.

Gender and Silence: The Private Grief of Men and Women:

In the Andaman and Nicobar Islands, as across the rest of India, suicide is not just a mental health issue—it is also a gendered issue, with 72.25 percent of all suicides being committed are by men on the islands. This stands similar to the national average of 72.5 percent. Women on the islands make up 27 percent of all suicides, while transgender individuals make up 0.2 percent of all cases.

At the outset, this may seem to be rooted in the traditional gender roles that men are supposed to follow in our society–being providers, the protectors, the stoic warriors who never falter. In keeping up with that role, men forget to take care of their mental health, which has drastic consequences. However, looking closely into the reasons for suicides gives us more answers.

'Depression and Loneliness' is the leading cause of suicide for both men and women, followed by family problems and illness and disease.

Therefore, both men and women deal with the same stress factors, which can lead to suicide in the end. However, for men–added causes of alcoholism, financial stress, and anger issues are prevalent. This may also be the reason for more suicides among them. Mental health and family counselling are crucial for saving the situation.

Data for transgender individuals is scanty. Though official records do not reflect causes of suicides for these cases, it can well be imagined that issues of societal seclusion, boycott and lack of sex-reassignment therapies on the islands may well have been contributors to the suicides.

Work and Worth: Rethinking Occupational Risk in the Andaman and Nicobar Islands

Looking at the professional profile of workers in the Andaman and Nicobar Islands gives us important insights. Of all suicides, a staggering 44.6 percent were by private sector employees, which includes salaried workers. The second most vulnerable section is housewives at 14.33 percent of all suicides. This is followed by students at 13.18 percent followed by government workers at 10.6 percent. Daily wagers come next at 8.59 percent of all suicides, followed by both old-age persons and farmers at 3.15 percent each. Only about 1.71 percent of all suicides are attributable to business persons. Unemployed persons come last, with only 0.05 percent of all suicides being committed by the segment.

This presents an intriguing picture. It is not the financially vulnerable sections, such as daily wagers, farmers, and unemployed persons, who are most vulnerable to suicides in the Andamans. In fact, salaried persons make up most of the suicides. Private workers and Government employees combined make up 55.2 percent of all suicides. This reflects how the issue of suicides on the islands is not a financial one-it may be deeper and more personal than that.

Comparing these statistics gives us insights into which occupational sections are most vulnerable to suicide on the Andaman and Nicobar Islands as compared to the national average. Suicides amongst government servants are 10 times the national average, while suicides amongst the private salaried class are 5 times the national average. If self-employed and

private professionals are combined, still, Suicides in Andamans amongst them are twice the national average. Suicides amongst old age persons are 3.5 times the national average. In other words, government servants are most vulnerable to suicides in the Andaman Islands followed by the salaried class and old age persons. These three occupational segments form the most vulnerable segment to suicides in the Andamans, as compared to the national average. Suicides amongst students is marginally higher in the islands at 11.35 percent of all, as compared to 8 percent at the national level. Housewives are equally worse off- Forming the second most suicide prone segment in both the Andaman and Nicobar Islands and the nation.

Does each occupational segment have a different set of causative factors leading to suicide? Let us have a look. Private workers, forming 44.6 percent of all suicidal persons, suffer from family issues, followed by depression and loneliness, alcoholism, and illness. For Government employees, who make up 10.6 percent of all suicides, the same top causes hold true, in addition to anger and stress. Housewives who make up 14.33 percent of all suicides deal with depression, followed by family issues as the primary cause. This means that if the worst-off occupational segments have to be uplifted, family counselling and mental health camps need to be made accessible.

On the other hand, Students–making up 13.18 percent of all suicides, suffer from anger issues, followed by failed love affairs, leading to suicide. School and college-level anger-management classes and mental health counselling is clearly missing on the islands. The lack of geriatric and palliative care on the islands can be gauged by the fact that old age, persons–forming 3.15 percent of all, are suiciding due to illness, followed by the death of a close Person. Meanwhile, financial issues followed by depression, and family issues, are causing business persons-making up 1.71 percent of all suicides.

Interestingly, some occupational segments are doing better in the Andaman Islands as compared to the rest of India. Suicides amongst daily wagers are roughly one-third of the national average, and this segment forms 8.59 percent of all suicides. Depression followed by family issues, alcoholism, illness, and failed love affairs are the top causes. Suicides

amongst Farmers are half the national average, and Suicides amongst the Unemployed are only 0.59 percent of the national average. Unemployed persons, making 0.05 percent of all, are committing suicide due to unemployment, followed by anger.

Basically, in the Andaman and Nicobar Islands, financially better-off persons (both government personnel and private salaried classes), with more elaborate safety nets, are more vulnerable to suicides, with the exception of old-age persons, who are committing suicides due to illness and the death of close ones. This signifies an utter lack of mental healthcare facilities on the islands, and calls for action. On the other hand, for government servants–whether the issue of leaves, transfers, and posting policies could be tweaked to help their cause–needs to be explored.

On the other hand, financially vulnerable sections like farmers, daily wagers, and unemployed persons are much less prone to suicides than salaried, financially secure persons. This may be due to tighter-knit families and social bonds, which help them sail through. Additionally, with rainfall being aplenty, and farmers engaging in high-value crops, farmer suicide due to non-realization of crop value in the market does not happen. Primary produce is arecanut and coconut, which have a secure foreign market. With a booming tourism industry, many farms simply supply local hotels and resorts with their produce at a good price. The farmer, hence, does fairly well here. It is pertinent to mention that most of the current farmers are displaced tribals who were given land and ration by the government and settled in non-flood/tsunami-prone areas. Today, this section of society is doing fairly well, at least when it comes to mental health.

The Emotional Geography: Where You Live Shapes How You Feel

As explored in the literature review segment, geography affects psychology in many ways. This has an impact on suicide too, among other things.

The Andaman and Nicobar Islands suffers from double-layered isolation—not only are communities within the islands scattered and often

hard to access, but the islands themselves are hundreds of kilometers away from the Indian mainland. This creates several logistical challenges in providing basic necessities like healthcare, education, and employment opportunities. This results in a population that is distant from the basic amenities and support systems typically available in the rest of the country. With a safety net missing, feelings of despair must naturally increase. To compound the situation, the local economy is largely seasonal, being fishing and tourism. This creates further economic uncertainty. These factors may increase the feeling of being driven to the wall, leading to suicide.

Disaster-prone areas also experience strains of their own kind. When the Tsunami struck in 2004, many tribal communities of the Andaman and Nicobar Islands were forced into the mainstream. Those living in the lowlands were moved out by the government, handed farming land, and a fixed stipend. Suddenly, people who had spent their lives in the wilderness–hunting to eat and swimming in the lap of nature–found themselves in alien lands, confined to small apartments. According to sociologists who have known the area for some time, this alienation of tribal communities from their older way of life led to increased incidents of depression. On the other hand, material well-being grew many-fold. Without the rigours of their previous life, and with a fixed income assured, these communities became well-off, often acquiring land as well as government jobs. As a result, the next generation of these tribal settlers grew up entitled. Many a suicide among young adults can today be seen attributable to trivial things such as being denied an iPhone by parents, not being allowed to go out with friends.

Let us explore the geographical distribution of suicides in Andaman and Nicobar islands. South Andaman is the epicenter of the suicide crisis, accounting for a staggering 84.49 percent of all suicide cases and a suicide rate of 51.09 persons per 100,000 persons. This is roughly 4 times the national average. This is slightly paradoxical because South Andaman, housing the Capital Sri Vijayapuram in it, is the most developed district in the Union Territory. Not only does it have better education and healthcare facilities, it is also the hub of tourism, which brings in steadier incomes.

All this forces us to confront a paradox–Material well–being does not guarantee emotional security.

By contrast, North and Middle accounts for only 8.3 percent of all suicides, with a suicide rate of 11.42 per 100,000. rise. Nicobar accounts for 7.3 percent of all suicides. The sub-archipelago has a suicide rate of 29.44 per 100,000 placing it between the extremes of South Andaman's urban anxiety and North Andaman's community stability. But Nicobar's reality is more layered and culturally distinct. Home to indigenous tribal communities, the Nicobar has witnessed a more drastic social transition than any other island community. Having been relatively isolated from the rest of the islands as well as the mainland, the Tsunami of 2004 led to a major change in its society. The government shifted out local inhabitants of the islands and settled them in flood-safe zones in other parts of the archipelago. These people–used to hunting–gathering-were given land and a stipend to settle them in their new life. This newfound prosperity didn't do well for the mental health of the Nicobarese. Away from their native homes and getting settled into an alien sedentary lifestyle may have led to emotional dissonance, which ultimately reflects in such a high suicide rate. Looking closer gives us the same idea. In the South Andamans, the leading causes of suicides include depression, followed by family issues and then illness and disease. North and Middle Andamans follow the same pattern, except that one-sided love affairs are an added cause. On the other hand, in the Nicobar family issues are the primary cause of suicides. This corroborates our narrative.

Hence, looking at suicides in Andaman and Nicobar Islands closely-based on parameters of age, sex, marital status, occupation, and geographical location-gives us a picture of how layered the problem at hand really is. There can hardly be a one-size-fits-all approach to solving it. Only by dealing with the issue at a granular level can the government move towards normalcy in a UT which has the second-highest suicide rate, and some of whose districts suffer from a suicide rate several times the national average.

But, before we move towards a possible solution to the issue at hand, let us discuss some problems faced while undertaking this study. Solutions to these issues may form the first stepping stone to a solution.

Problems Encountered: The Data Dilemma

During the course of this study on suicides in the Andaman and Nicobar Islands one of the most pressing challenges encountered was the quality, structure, and consistency of data maintained by the SCRB. While the dataset contained 1,048 suicide records over several years, the true analytical value of these records had multiple shortcomings.

1. Inconsistent Categorization and Oversimplification:

The first and perhaps most glaring issue was the inconsistent and overly generalized categorization of causes of suicide. Categories like "depression," "family issues," or "sickness" were used frequently and with little clarity on what they actually meant in each case.

For instance, the category of "depression" has been used in a very loose fashion as a catch-all term. Clinical depression is one thing, and sadness another. This kind of vague tagging dilutes the specificity that is vital for understanding suicide patterns. A person suffering from familial neglect may be sad and commit suicide. But recording the cause as ‘Family Issues’ is the correct thing to do, instead of using the blanket ‘Depression’. Similarly, an elderly person ailing of a disease may commit suicide out of a sense of despair due to a lack of medical facilities. However, recording the cause of suicide as ‘Depression’ instead of ‘Disease’ may not bring out the picture clearly.

This usually happens because police personnel conducting an inquest are not properly briefed about the significance of recording the causes with accuracy. Alternatively, it is usually much easier to use a blanket word than apply one’s mind to record the correct underlying cause.

2. Missing Variables: The Gaps that Hinder Insight

The absence of key socio-economic and demographic variables further complicated any attempt at robust analysis. Important indicators like income level, nativity (whether the deceased was a native islander or a

migrant), educational background, employment status, and previous mental health history were either missing or haphazardly entered.

Knowing these variables are not just academic luxuries—they are vital signposts in understanding the phenomenon of suicides. For example, by studying suicide is prevalent among which class of people, a targeted approach to the issue of suicide can be created. Similarly, knowing about the mental health history of a person could help improve early identification and create tailor-made programs to prevent them. Furthermore, information about the location of the suicide—whether it occurred at home, in the workplace, or in a particular public area—could help us create location-specific strategies for suicide prevention.

Implications for Policy and Intervention: Building a Smarter, More Empathetic System

The findings of this research, drawn from SCRB as well as First Information Reports (FIRs), ground-level interviews, and cross-sectoral consultations, reveal the scope of the suicide crisis in the Andaman and Nicobar Islands and highlight the critical need for targeted, compassionate, and data-driven policy interventions. With limited resources, the Police, as well as the Civil department of the government, do their bit in suicide prevention and care, like Mental Health Melas. However, if the interventions are generic and untargeted, then those limited resources may be as good as wasted. A targeted approach is needed not just to alleviate the issue at hand but also for the sake of administrative efficiency. But policy is as good as the data that informs it. If the data is generic, then the interventions built upon it will be equally flawed. With the current state of data on suicide in Andaman and Nicobar Islands all efforts at creating targeted responses will be frustrated.

In view of the above, the following recommendations are framed to address systemic gaps while centering the emotional and social needs of the islanders.

1. Revise the Unnatural Death (UD) Proforma:

The **Unnatural Death (UD) proforma**, which is used to record details of suicides and other non-natural deaths, is a form built for documentation,

not analysis or preventive foresight. This proforma needs an overhaul if we seek to have more informed decision-making. The area prescribed for recording the Cause of Suicide is often filled with blanket words like 'Depression' by the inquest officer. This hides more than it reveals. In other cases, mis-categorising of reasons also happens, which gets clarified only when one reads the detailed note.

The room for such subjectivity needs to be removed-and for this, the UD proforma needs to be redesigned. It must include structured tick-boxes listing all the causes of suicides, so that there is less room for subjectivity and mis-categorisation by the inquest officer. To target policies better at specific classes and demographies, socioeconomic indicators such as income levels, education level, etc, must be recorded. Additionally, the proforma must also include room for recording risk factors such as recent bereavement, unemployment, substance abuse, or domestic violence or a history of mental health issues.

Keeping these points in mind, the author has designed a sample UD Proforma. The same is attached at the end of the paper.

2. Train Data Entry and Investigative Staff:

A system cannot function well without well-trained people who understand how to run it properly. In our context, police personnel as well as SCRB staff must be trained in understanding the nuances of suicide reporting and why this is needed, especially in the context of the Andaman & Nicobar Islands. This may include mental health professionals. This component of training may be included in the periodic training modules that already happen. Investigating officers must learn the art of probing intelligently for underlying emotional, social, or economic factors of suicide and only then record the facts of the case with accuracy.

3. Data-Driven Policymaking: Knowing Who, Where, and Why

Reliable, granular, and regularly updated data is the backbone of any responsive mental health policy. This study has already highlighted major deficiencies in current suicide data practices in Andaman and Nicobar Islands. To remedy this, institutionalisation of data collection and analysis must be done. Suicide cases must be segregated by age, gender,

occupation, nativity, geography, known triggers etc. for analysis. To respect data privacy, datasets may be anonymized and shared with research institutions to design better interventions. This data may give critical insights into emerging suicide risk patterns and hotspots.

Data audits at the SCRB must be conducted on lines of financial system audits to prevent misreporting, and maintain data quality ie. fill gaps and ensure uniformity. This can be done quarterly or biannually. This should ideally be carried out by a team comprising both Police and Administrative officers, along with mental health experts.

4. Suicide Prevention Cell: Institutionalizing a Life-Saving Mission

A dedicated Suicide Surveillance and Prevention Cell within the Police Department is essential for monitoring and preventing suicides. This may include a 24/7 suicide prevention helpline staffed by personnel having some training in mental healthcare. This cell may also be nodal in compiling real-time data on suicide attempts and deaths, analyzing trends, and coordinating emergency response. It may be used to create regular policy briefs on the issue of suicide in the Andaman and Nicobar Islands. A collaboration may be made with the Directorate of Health Services, NGOs, school authorities, and the Panchayati Raj institutions.

5. A case for Comprehensive Community Outreach:

The idea that suicide is an option needs to change. In a society that so easily resorts to suicide, little can be achieved through clinical measures alone. The police and administration need to raise the value of life in the eyes of people, which can be done via outreach to suicide prone pockets. This can be done by conducting outreach programs in schools, colleges, and suicide-prone pockets.

The more targeted, the better. For instance, this study enumerates the causes of suicides for each age group and occupational segment. The outreach programs can target these causes for programs targeted at each of these segments. For instance, among government servants, family issues are a prominent cause of suicides. Family Counselling camps can be held in Police Melas for these persons. Among the youth, anger and broken love relations are a cause for suicides. Anger Management Camps, Peer Support Clubs, Career Counselling for them may be a good option. The

incorporation of technology can also take it all forward with the likes of mood-tracking apps or anonymous Q&A forums for those who may hesitate to speak face-to-face. On the other hand, if the elderly are suicidal due to illness and old age, Medical Camps and Mental Health camps may be held, especially targeted at them. Short-duration Emotional Resilience Training programs may be held in these outreach programs for the general public. A tie-up may be done with mental healthcare professionals in the GB Pant Hospital and the like.

Conclusion: From Numbers to Lives

The Andaman and Nicobar Islands offer possibly the most mood-lifting sights in all of the country, reflected in the increasing number of tourists visiting the islands every year. How contrary, then, that natives of these islands must suffer silently and give up on their lives so easily.

The suicides studied in this report were not random acts. They are rooted in deeply structural, cultural, emotional, and psychological vulnerabilities. The Police department's responsibility lies in ensuring the safety of lives. In a place where the silent pandemic of suicides is taking such a heavy toll on those very lives, it is the moral imperative of the department to take informed and proactive action on the issue.

What is needed is a conscious acknowledgement of the issue and redirection of policy at each level- both in the Police as well as the Civil Administration, to ensure suicide prevention. Grandiose programs that merely end up being photo-ops are not needed, nor are they recommended to serve the purpose. Thoughtful interventions, instead, would go a long way to ensuring that people of the Andaman and Nicobar Islands see the value of life, and get the necessary support when life seems low.

The paper presents certain recommendations, which, if followed, stand to make the Andaman and Nicobar Islands a model for sensitive, inclusive, and data-backed governance in remote and underserved regions. In doing so, the administration would not only prevent loss of life, but also shape a society where emotional well-being is treated not as a luxury, but as a shared responsibility. With three times the national average suicide rate, it is time the islands healed into robust and happier living.

References:

1. *Cavanagh, J. T. O., Carson, A. J., Sharpe, M., & Lawrie, S. M. (2003). Psychological autopsy studies of suicide: A systematic review. *Psychological Medicine, 33*(3), 395–405. https://doi.org/10.1017/S0033291702006943*
2. *Canetto, S. S., & Sakinofsky, K. (1998). The gender paradox in suicide. *Suicide and Life-Threatening Behavior, 28*(1), 1–23.*
3. *Colucci, E., & Lester, D. (2012). *Suicide and culture: Understanding the context.* Hogrefe Publishing.*
4. *Dandona, R., Kumar, G. A., Dhaliwal, R. S., Naghavi, M., Vos, T., Shukla, D. K., & Dandona, L. (2020). Suicide mortality in India: A nationally representative survey. *The Lancet, 399*(10332), 2343–2351. [https://doi.org/10.1016/S0140-6736(20)30453-1](https://doi.org/10.1016/S0140-6736%2820%2930453-1)*
5. *Das, A. (2025, January 5). Interview with Medical Officer, GB Pant Hospital. Conducted by Anna Sinha, Port Blair. [Personal interview].*
6. *Dube, S. R., Anda, R. F., Felitti, V. J., Chapman, D. P., Williamson, D. F., & Giles, W. H. (2001). Childhood abuse, household dysfunction, and the risk of attempted suicide throughout the life span: Findings from the Adverse Childhood Experiences Study. *JAMA, 286*(24), 3089–3096. https://doi.org/10.1001/jama.286.24.3089*
7. *Durkheim, É. (1897). *Suicide: A study in sociology* (J. A. Spaulding & G. Simpson, Trans.). Free Press.*
8. *Hirsch, J. K. (2006). A review of the literature on rural suicide: Risk and protective factors, incidence, and prevention. *Crisis, 27*(4), 189–199.*
9. *Isaac, M., Elias, B., Katz, L. Y., Belik, S. L., Deane, F. P., Enns, M. W., Sareen, J., & Swampy Cree Suicide Prevention Team. (2009). Gatekeeper training as a preventive intervention for suicide: A systematic review. *Canadian Journal of Psychiatry, 54*(4), 260–268. https://doi.org/10.1177/070674370905400407*
10. *Joiner, T. (2005). *Why people die by suicide.* Harvard University Press.*
11. *Kleiman, E. M., & Liu, R. T. (2013). Social support as a protective factor in suicide: Findings from two nationally representative samples. *Journal of Affective Disorders, 150*(2), 540–545. https://doi.org/10.1016/j.jad.2013.01.033*
12. *Mann, J. J., Apter, A., Bertolote, J., Beautrais, A., Currier, D., Haas, A.,*

*Hegerl, U., et al. (2005). Suicide prevention strategies: A systematic review. *JAMA, 294*(16), 2064–2074. https://doi.org/10.1001/jama.294.16.2064*

13. *Meena, M. K. (2024, December 15). Personal interview conducted by Anna Sinha, Port Blair, Andaman and Nicobar Islands.*
14. *Mondal, S. (2024, December 28). Interview with local police constable, Aberdeen Police Station. Conducted by Anna Sinha. [Personal interview].*
15. *National Crime Records Bureau. (2023). *Accidental deaths & suicides in India, 2018–2022.* Ministry of Home Affairs, Government of India.*
16. *Patel, V., Ramasundarahettige, C., Vijayakumar, L., Thakur, J. S., Gajalakshmi, V., Gururaj, G., Suraweera, W., Jha, P., & Million Death Study Collaborators. (2012). Suicide mortality in India: A nationally representative survey. *The Lancet, 379*(9834), 2343–2351. [https://doi.org/10.1016/S0140-6736(12)60606-0](https://doi.org/10.1016/S0140-6736%2812%2960606-0)*
17. *Pirkis, J., John, A., Shin, S., DelPozo-Banos, M., Arya, V., Analuisa-Aguilar, P., et al. (2021). Suicide trends in the early months of the COVID-19 pandemic: An interrupted time-series analysis of preliminary data from 21 countries. *The Lancet Psychiatry, 8*(7), 579–588. [https://doi.org/10.1016/S2215-0366(21)00091-2](https://doi.org/10.1016/S2215-0366%2821%2900091-2)*
18. *Platt, S. (1984). Unemployment and suicidal behavior: A review of the literature. *Social Science & Medicine, 19*(2), 93–115. [https://doi.org/10.1016/0277-9536(84)90276-4](https://doi.org/10.1016/0277-9536%2884%2990276-4)*
19. *Racine, M. (2018). Chronic pain and suicide risk: A comprehensive review. *Progress in Neuro-Psychopharmacology and Biological Psychiatry, 87*, 269–280. https://doi.org/10.1016/j.pnpbp.2017.08.020*
20. *Roy, S. (2024, December 22). Interview with NGO field coordinator, Pratigya Foundation. Conducted by Anna Sinha, South Andaman District. [Personal interview].*
21. *South Andaman District Police. (2025). *First Information Report (FIR) records on suicide cases, 2018–2022.* Unpublished internal records, accessed November 2024–January 2025.*
22. *World Health Organization. (2014). *Preventing suicide: A global imperative.* World Health Organization.*
23. *World Health Organization. (2021). *Suicide worldwide in 2019: Global health estimates.* World Health Organization.*
24. *Zalsman, G., Hawton, K., Wasserman, D., van Heeringen, K., Arensman, E., Sarchiapone, M., Carli, V., et al. (2016). Suicide prevention strategies*

*revisited: 10-year systematic review. *The Lancet Psychiatry, 3*(7), 646–659. [https://doi.org/10.1016/S2215-0366(16)30030-X](https://doi.org/10.1016/S2215-0366%2816%2930030-X)*

Andaman and Nicobar Islands Police
Tentative Proforma for Reporting Unnatural Deaths

1. SL No. _____
2. Name of District _____
3. Police Station _____
4. UD FIR No. _____
5. Date _____
6. Name of Deceased _____
7. Nativity (Tick from below)
   - 7.1. Bengal
   - 7.2. Tamil Nadu
   - 7.3. Kerala
   - 7.4. Bihar/Jharkhand
   - 7.5. Others (Please specify) _____
8. Male/Female/Child _____
9. Age of Deceased_____
10. Occupation (tick from below)
    - 10.1. Daily Wager
    - 10.2. Private worker
    - 10.3. Business owner
    - 10.4. Government Employee
    - 10.5. Home Maker
    - 10.6. Student
    - 10.7. Unemployed
    - 10.8. In case of child, also mention occupation of Father and Mother_____

11. Monthly Family Income (approx.)_____
12. Suicidal/ Accidental _____
13. Mode of Death _____
14. Place of Occurrence_____
15. Cause of Death (Choose from below)
    - 15.1. Alcoholic addiction
    - 15.2. Disease/Illness
    - 15.3. Death of Close person
    - 15.4. Psychiatric Problem/Depression under treatment
    - 15.5. Family disputes
    - 15.6. Marital discord
    - 15.7. Extra Marital Affairs
    - 15.8. Financial Issues
    - 15.9. Love Affair/One sided love
    - 15.10. Unemployment
    - 15.11. Anger/Decision of Passion

16. Past behaviour of the deceased (whether any behavioural change was noticed/past history of any conflict etc.)

_____

_____

_____

_____

17. FR Number
18. FR Date
19. Occupation
20. Marital Status
    - 20.1. Married
    - 20.2. Unmarried
    - 20.3. Widow
    - 20.4 widower

Author's Profile

Anna Sinha is an IPS Officer of the 2022 batch, borne on the AGMUT Cadre. She is currently posted as ASP, Special Operations Group, Srinagar, Jammu & Kashmir. She was a JRF Scholar of Economics, and has done her M.A. Economics from Ambedkar University Delhi, and B.A Hons. in Economics from Ramjas College, University of Delhi.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P. 90-96)

Drones and Policing

Deepak Krishna*

Drones or UAVs have become part and parcel of daily life in current time. Drones are unmanned aerial vehicles/objects which are flown from a source for a specific purpose.

Drones are being used extensively for varied functions. Drones are used in reconnaissance, follow-up/pursuit of criminals & offenders and public safety purposes. Military uses UAVs/Drones for reconnaissance, offensive & defensive operations and been using since Kargil war in 1999. Drones were also used by the IAF and the Navy across the globe for finding and destroying enemy RADARs. They are being used by civilians for photography and survey purposes. Drones are also used to survey land areas damaged during devastating flood in Uttarakhand in June 2013 & rebuilding "Uttarakhand".

Definition:

Drones more formal name is Unmanned Aerial Vehicles (UAV). A drone is a flying Robot. The aircraft may be controlled or can fly autonomously with the help of software-controlled flight plans in their embedded systems that made in conjunction with GPS.

Uses of Drones:

- Target and decoy providing ground and aerial gunnery a target stimulating an enemy aircraft or missile.
- Reconnaissance to provide battlefield intelligence.

* *Deputy Commandant, 47 BN SSB, Raxaul (Bihar).*

- Combat to provide attack capability for high-risk missions.
- Logistics and delivering cargo.
- R & D advancement of UAV Technologies.
- Civil & Commercial UAVs in the field of agriculture, aerial photography and data collection.
- Policing in hot pursuit of offenders.

Types of Drones:

Drones can be classified on the basis of their usage as under:

1. Civilian Drones: Which are used for civil research, development purposes and other commercial usage. such as photography, mapping, agriculture, delivery and disaster management.

2. Military Drones: UAVs which are used for recce, finding enemy RADARs & combat purposes are known as Military Drones.

Civil Drones in India:

These drones are being used to assist in a services ranging from disaster relief, aerial photography and security & surveillance.

In the year 2013, during disaster relief operations in Uttarakhand after severe flooding, the social drones' civil drones were used for areas that were deemed unsafe for conventional relief methods and also for areas where relief efforts had been stalled. Following startups of Indian companies in UAV field are notable.

(1) Airpix: Specialised in aerial photography and video production. Real estate agents, tourism organizations, journalists in disaster zones etc are potential clients of Airpix. After flood havoc of June 2013 in Uttarakhand, Airpix drone photography proved helpful on a campaign to rebuilt Uttarakhand. It also spreads awareness regarding infrastructural deficiencies in the mountainous state.

(2) Garuda Robotics: It was started by 20 year old Pulkit Jaiswal. Garuda produces software that gathers & analyse data collected by drones. The software to control unmanned aircraft is also produced by the company. Garuda markets the products for various usages ranging from land and agricultural surveys to security, search, rescue and logistics.

(3) Edall Systems: A Bangalore based company providing engineering, design & manufacturing services. It is also involved in the Drone development & UAV training programmes for use of students & professionals. The company also builds parts for India's National Aerospace labs & DRDO.

Military Drones in India:

During the 1999 Kargil war with Pakistan, India for the first time used military drones. Manned English Electric Canberra PR57 aircraft for photo reconnaissance along the LOC was deployed by the Indian Air Force. However, over the mountainous Kargil terrain this system proved highly inefficient & weak, strategically. After losing Canberra PR57 to Pakistani infrared homing missiles by India, IAI Heron and Searcher drones were discreetly supplied to the Indian Air Force by Israel. They proved quite useful in acquiring target information along the Line of Control.

Presently India's arsenal includes the Israel Aerospace Industries Harpy and Harop Unmanned Combat Aerial Vehicles also IAI Searcher and Heron UAVs.

S. No.	Type	Class	Role	Notes
1.	IAI Harpy	Israel	Attack	A small UCAV capable to home into enemy RADAR emissions, thereby destroying both itself and enemy RADAR system. In service with the IAF.
2.	IAI Harop	Israel	UAV	A small UCAV capable to home into enemy RADAR emissions, thereby destroying both itself and enemy RADAR system. In service with the IAF.
3.	IAI Heron	Israel	Surveillance	In service with IAF and Indian Navy.

4.	IAI Searcher	Israel	Surveillance	In service with Indian Army.
5.	DRDO Nishant	India	Surveillance	In service with Indian Army.
6.	DRDO Lakshya	India	Aerial target	A small target drone, which is in service with IAF and Indian Navy.

In late 2013 Israel Aerospace Industries (IAI) and India's Defence Research & Development Organisation (DRDO) offered to jointly develop a newer version of the Heron UAV.

In June 2013 deployment of Heron surveillance drones was started by India over Maoist rebel strongholds in the East in a limited capacity. This type of activity was limited to Andhra Pradesh, Odisha & Andhra-Chhattisgarh. The UAVs have not been of major use in Recce and Surveillance as these states are densely forested.

India's DRDO has also developed its own domestic UAV programme. Below is a list of DRDO drone projects:

1. DRDO Lakshya: A target drone which uses solid propellant rocket motors for its launch and is sustained by a turbojet engine in flight. It serves for discreet aerial reconnaissance and target acquisition.

2. DRDO Nishant: Primarily designed for intelligence gathering over enemy territory and also for recce target designation, training, surveillance, artillery fire correction and damage assessment are some other uses.

3. DRDO Aura: It is a stealth drone that can release missiles, bombs and precision guided munitions.

4. DRDO Rustom: Modelled after the American predator UAV, it is a Medium Altitude Long Endurance (MALE) system. Rustom is used to serve for both recce and combat missions.

Worldwide Drones Usage in Modern Warfare:

In today's warfare the drones/UAVs are no more limited to their earlier role of reconnaissance and target location. However, they are used in very complex and new ways to hit the enemy hard where it hurts the most. Civilians are losing their lives and many vital installations are targeted by

using drones deep inside enemy territory beyond the border is the latest type of warfare the world has seen off late. Ukraine targeted Russian airbases using drones carried on a Trailor discreetly. In 2025 around three quarters of all Russian casualties have been as a result of Ukrainian drones. At sea, Ukraine has used drones to attack multiple warships and break the Russian Navy's Black Sea blockade, forcing Putin to withdraw the bulk of his remaining fleet from Russian-occupied Crimea.

Israel is using quadcopter drones to intimidate and terrorise people in Gaza Strip. Israel uses drones, also called "death drones", to drop explosive, drop pamphlets and announcement purposes to contain Palestinian people in a limited area. Israeli quadcopter drones are carrying machine guns and grenade launchers which are targeting even children in Gaza is the latest abuse of modern technology drones. ELBIT Systems is the company of Israel which designs, innovates, and builds modern technology drones with AI-powered systems. AI has massively enhanced the speed, precision, and load-carrying capacity of drone systems.

Police Drones in Service:

Police forces worldwide are using drone technology for various purposes and operations as enumerated below :

1. Recce and pursuit of a target.
2. Dropping life jackets in flooded areas for public safety.
3. Dropping medical & food items to isolated areas.
4. For night-time searches.
5. Real-time data streaming of unreachable far-flung areas.
6. Monitor traffic and control.
7. Identifying road conditions and traffic violations.
8. Search and rescue operations.
9. Fire-fighting exercises.
10. Reporting incidents in a city.
11. Tracking suspects in rogue vehicles.
12. Patrolling crowded areas/crowd monitoring.
13. Surveying crime scenes and evidence.
14. Pursuing high-speed car chases.

15. Tactical support.
16. Emergency response coordination.

Types of Drones Police forces Using Worldwide:

1. **RMUS Heavy Duty Police Drone**: Designed by US, Flight time of 56 minutes, high-resolution cameras, thermal sensors.
2. **Autel EVO MAX 4T**: Crime scene investigation, Anti-jamming capability, mobile recce, obstacle avoidance capability.
3. **DJI Matrice 350 RTK**: It moves silently and stealthily, gathers intelligence and monitors suspect.
4. **Parrot ANAFI USA:** Quite and rugged, small in size, advanced optics and zoom, ideal for night operations with thermal capabilities, usable from -36^0 C to 56^0 C temperature range. US Navy uses Parrot ANAFI and also used for purposes of wild fire operations, maritime surveillance.
5. **DJI M30 Series**: This drone is compact, rugged, ready in a moment for operations, AI assault trekking. It uses laser range finder that measure distances of targets, high-resolution cameras and can work in thick vegetation forests.
6. **Skydio X 10** – **California, USA:** It can be air borne in 40 seconds, 7.5 miles flight distance, 40 minutes fly time, speed of 36 miles per hour, thermal cameras for night-time searches. It is used in crime scene investigation by police.
7. **DJI Mavic Mini 2** : 249 grams, 13 cm long. It can fit in your palm. It can fly at a speed of 57 km/hour and reach altitude up to 4000 metres, 31 minutes flight time and transmission up to 10 km. It is used by Qatar Traffic Police Department.
8. **Autel EVO Lite Enterprise** – Lightweight UAV. Airborne up to 40 minutes, 50 MP camera, used in post-incident analysis, real-time arial feed from the area, automatic "return to home" facility. Used by **Los** Angels Police Department.
9. **Yuneec Typhoon H**: 1.9 kg weight, a Hexacopter, 70 km/hour speed, 28 minutes fly time, used by **South Wales Police**, **UK** for crowd monitoring.
10. **HYBRIX 20**: **Spain police** use this drone, 13 kg weight, 20 km per hour speed, 02 hours flight time, used in complex terrain.

Desirable Features in a Police Drone:

1. Power, precision and speed.
2. High-resolution thermal cameras with zoom-in facilities and 4K feed for taking considered decisions by police forces.
3. Better payload carrying capacity for supplying food, blankets, life jackets, medicines etc in stressed areas.
4. Good quality thermal sensors for identifying hidden suspects using fire for cooking or smoking.
5. AI powered onward object trekking.
6. Autonomous navigation system with obstacle avoidance.
7. Return to home feature.
8. Maximum number of targets the drone can monitor.
9. Anti jamming capability in signal hostile areas.
10. Maximum flight time and battery capacity.
11. Weather protection from rain, snow and temperature.
12. Data storage and transmission capability.
13. Night time operability & quality of thermal cameras.
14. Altitude a Drone can reach and function without failure.
15. Higher transmission rate in kms helps operate far from the pilot.

In todays time drone technology is getting advance day by day and becoming integral part of police forces in order to function more efficiently and apprehend culprits and perpetrators. Dedicated Drone Cells and a R & D teams must be established for overseeing advancement of drone technology in police forces for their specific needs. It would be just to call tomorrow a Drone era.

Author's Profile:
Deepak Krishna, Deputy Commandant, 47 BN SSB, Raxaul (Bihar)
The educational qualification: Graduate in Arts.
Officer has joined the SSB as Assistant Commandant vide CPF, UPSC.
Experience in Human Resources and Security.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P. 97-108)

Digital "Stop and Frisk": Predictive Micro-Behaviour signal of Online Users for Pre-emptive Policing Checks

Lakshya Sharma* & Dr. Sachiv Kumar**

Abstract:

In this paper, the new trend is explained and the term Digital Stop and Frisk is used, which is a form of anticipatory cyber-policing with the use of sophisticated artificial intelligence (AI) algorithms that can identify possible cybercriminal activity prior to an actual crime. Based on the behavioural biometrics scheme, digital stop-and-frisk captures micro-behaviours like anomalies in the pace of cadences of keystroke in network traffic cognitive loads or switching pattern behaviours that are not within a standard scheme which could indicate the intention to commit a cybercrime. The examination of these signals at any given time avails intervention in opportunities before crimes have been engaged thereby a change in reactive policing to proactive models in the area of digital security in which Policing is geared towards forestalling cybercrime even at the reconnaissance stage within which supposed offenders would appear to have done nothing by other than probing systems or planning attacks. It employs a predictive analytics engine to issue warnings on any irregular activity of the user like the navigation anomalies, credential

* *Mr. Lakshya Sharma, Teaching Associate in Lal Bahadur Shastri National Academy of Administration, Mussoorie.*

** *Dr. Sachiv Kumar, Faculty of Law, in Lal Bahadur Shastri National Academy of Administration, Mussoorie.*

stuffing patterns, and associations to risky dark net marketplace sites. This is a curious comparison since, although A Digital Stop-and-Frisk may prove highly efficient in preventing cybercriminals and preserving the safety of a would-be victim, there lie profound grounds that are ethical, legal, and surrounding privacy. The most fundamental issues include firstly, the violation of digital privacy; secondly, the fact that algorithms can be biased to produce false positives; and, lastly, this whole machine could be another tool of mass surveillance against people against their knowledge and understanding and even without their permission however it is un the interest of public service. This paper has a techno-legal context and a consideration of the ethical implications of predictive micro-targeting in cyber policing as it argues that fair and accountable regulations be explicitly stipulated on the concept of fairness and accountability. Being properly controlled, digital stop-and-frisk may be useful in shielding one of the essential strata without causing unnecessary hazard due to the verification of unwarranted surveillance, further utilising its capabilities significantly to decrease cybercrime.

Keywords:
Digital Stop-and-Frisk, Predictive Policing, Behavioural Biometrics, Cybersecurity, Ethical Concerns.

1. Introduction:

The modern world of the cyber is an outgrowth of a convergence of digital platforms, algorithms and data-driven interaction. With much of social life shifting to the World Wide Web, organised cybercrime has evolved-between occasional activities of individual opportunistic hackers through to the activities of criminal groups functioning on multiple planes-as well. (Liu et al. 2017) Anonymity and encryption and infrastructural loopholes-everything the network depends on to remain afloat; are being applied to some crime escapades that cross all physical boundaries influencing the law enforcement agencies in their efforts to anticipate intent with more sophisticated types of computational tools. This tension promotes a redefinition of policing as pro-active rather than reactive in orientation with

only some milliseconds to be any reliable foundation on which any attack can be made and then quickly revert to the virtual anonymity of a physical facade. The closest similar to the practice that happened in the modern world that is considerably comparable to the invention of reasonable suspicion-based stop-and-frisks, yet occurs online, is the concept of Digital Stop and Frisk. Digital stop and frisk in straightforward terms is a set of artificial intelligence programmes that indicate attempts on users, a behavioural process that sharply violates the norms of any conceivable window that indicates the possibility of cybercrime. A coin has the two sides, it is the onus of the owner, how he will give the heed. As opposed to the traditional programme that presupposes seeing a visible criminal activity to proceed with the implementation, Digital Stop-and-Frisk relies on minimal signs or suspicions perceived of a person; perhaps odd network traffic patterns among other possible detectors that remain under the scanner of more advanced AI models as amateurs in the role of a legitimate threat actor who could communicate with darknet markets. This paper examines the techno-operative structural logic and ethics debate of evolutionary net protection dynamical ecosystems requirements that such systems evolve or whether it puts in place a regime of algorithms as the digital watchdogs of the continuous state apparatus of criminological intelligence artificial analytical-informed perspectives on cybersecurity to digitally advanced critically holistic emergent levels. More precisely, this paper entails an analysis on two important levels:
(1) techno-operative structural logic; and,
(2) moral discussion on micro-targeting online policing.

2. Conceptual Framework: The Digital "Stop and Frisk"

Digital stop-and-frisk is an endeavour to recreate, using algorithms in virtual space, what physical policing has been performing for many years, with the eyes: identifying persons whose behaviour seems, at the first glance, to be suspicious. However, as the digital world lacks the physical cues on which suspicion may be built-there is not micro-behavioural telemetry that could build suspicion in the digital arena, as there is none of the overt and apparent gesturing or situational nuances in a physical space-

suspicion is constructed based on micro-behavioural telemetry as opposed to the overt gesture or circumstance of a physical one.

2.1 The Physical to Digital Stop-and-Frisk Evolution.

The physical stop-and-frisk has been relying on intuition of the cops, environmental indications, and behavioural abnormalities. Such interventions have been rationalised by the courts under the notion of reasonable suspicion that weighs against individual rights and safety to achieve an overall state interest in enabling such interventions. In this case, though, artificial instead of human intelligence would be required to conduct the synthesis of heuristics-of-suspicion since digital stop-and-frisk does not rely on bodily nearness, but on algorithmic nearer; the closeness of a user behaviour to models of known cybercriminals,

2.2 Pre-emptive Digital Cheques: The Operation.

Pre-emptive cheques are based on machine learning systems that continually consume and examine metadata of user activity, device fingerprints and network transitions, browsing patterns and switching behaviour to other platforms; interactivity to high risk space; time signature anomalies that evidence of obfuscation.

2.3 Behavioural Patterns of Cybercriminals.

Where the system identifies that the user behaviour has matched with the profile of known cyber-offenders, further authentication can be required of the user along with an automatic electronic alert or even a referral to an investigator. The process creates what can be termed as digital body language among individuals in cyber space and charts the elements of tension that may be similar to those of suspicious body behaviour. Hasty navigation patterns, scans in security borders, routing cycles of credentialing, sudden shifts in IP addresses and bursts of encrypted traffic are the micro-behavioural characteristics that the system mostly links to cybercriminals. Novice offenders leave unproductive and chaotic digital footprint and more skilled actors strategically create a signature conduct that hides their intent which makes the generation of early pattern traces of

possible future offences fascinating questions involving privacy controls and at what point should legitimate security actions turn into intrusion surveillance functions.

3. Artificial Intelligence Processes of Predictive Micro-Targeting:

Behavioural analytics like that with high level of resolutions can see anomalies and intents in the cyberspace activities that are well past the conventional way of digital forensics using pieces of evidence. In its predictive form, long afore an offence has been committed, it searches on incidences of behaviour; offence that only may be already contemplated. The artefacts now lie buried in what is becoming embraced as the subconscious or, as we might call it, behavioural biometric strata: keystroke rhythms, interface dwell time patterns, even cognitive load variability in the form of ostensibly random task-switching which can leave recognisable trace of itself to be detected by sufficiently developed artificial intelligence platforms. They are tiny behavioural pulses that are not visible to the eyes of human viewers but become massively evident in the hands of AI models trained on datasets of behavioural data such as TypingDNA or PyRIT. The anomaly detection systems are still a part of statistical inference and machine learning. They are however supported by cutting edge models of anomalies which incorporate isolation forests, auto encoders network or behaviour monitors using LSTMs open source as DeepLog anomaly detection system or transformerised behaviour encoders such as Behaviour GPT (Liu et al. 2017, Devlin et al. 2019) demonstrate how AI develops normal digital activity baselines and identifies user activities that slightly but predictably their normative paths. A novice cybercriminal presses the keys of his browser into a bomb and his exploration between various exploit manuals wild experimentation with repositories like XSStrike, sqlmap, AutoRecon may not be outright criminal activity but reflect the mental state of a user that skillfully bumps the bounds of exploration into exploitation. Their data streams are compounded in a few layers of network telemetry, device fingerprint, OS-level artefacts, cloud interaction logs, cross-platform identity drift artefacts

and so on. Telemetry correlation allows network devices to identify identities on a number of platforms, which are depicted in a family tree with openCTI, Malcolm, or Wazuh-AI. So suggested micro-targeting is not trivial watching and does not elevate arbitrary suspicions but is an analytically planned engine of inference of behaviour which is going to identify incipient forms of crime gestation out of the behaviour.

4. Applications and benefits of preemptive cyber-police:

The reality and operational value are the efficiency with which it can combat an assault at the reconnaissance-the stage when the majority of digital crimes can be detected. Most of the upper-end cybercrimes commence with some manner of probing: port scanning, vulnerability maps; network reconnaissance as in ReconSpider or theHarvester or AutoRecon (all three again also fully justified in their educational and security-testing applications). It is important when one is scanning a network of a school district methodically at odd hours or when the VPN IP addresses of VPNs appear to be switching very rapidly. It can be the very first indicators that could be identified by AI-of a ransomware mocking operation; investigative intervention will take place prior to the breach or extortion assertion becoming a reality. These tools are very useful in terms of the safety of vulnerable digital populations, other than the high-profile breaches. The AI sentiment and conversation analysis can deconstruct typical recognisable behavioural arcs employed by online groomers, manipulators, and digital predators using toxicity classifiers based on BERT, DeepMoji emotion analysers and levels, including levels of OpenAI moderation. Digital stop and frisk systems recognising the behavioural drift of a pseudonymous adult account with a minor in the initiation of boundary-testing conversations or employing typically escalated patterns of conversation in pressurising will prompt the implementation of protective intervention. The latter was originally written in English but found its way into other languages, including Japanese. (Devlin et al. 2019; Felbo et al. 2017) Predictive micro-targeting drives to automated behavioural risk scoring where artificial intelligence reconstructs heat maps of suspicious behaviour through contextualisation

of tools and not normal browsing paths, tool usage, mixing of cryptocurrencies behaviour, exploring darknet gateways and abrupt changes in digital identity. A person who suddenly starts to have interactions of a repository nature with such tools as BlackMamba-AI-Keylogger, Evilginx2 or complex ransomware-creator packages when accompanied with some metadata pattern of suspicious activities, may be a good candidate on a deep look list. Ultimately, digital stop-and-frisk equips the system with pre-emptive answers that are measured in magnitude like automated warnings, compulsory challenges of verification that are made a human-initiated outreach to the juveniles who are possibly making their way into the cyber-offending sub-culture. It is this model that a public health model would be, in the event that policing becomes more behavioural risk prevention before the damage, and less punitive after the damages.

5. Risks, Limitations and Ethical Challenges:

It is indeed a technological miracle, digital stop-and-frisk, but has immense ethical and legal issues, most of them due to the fact that the rights of our digital privacy are being eroded in silence and scarcely being registered but in the interest of public service, it should be done. It is effective in micro-behavioural signal tracking - unremitting monitoring of a large number of signals of which users themselves are oblivious and which they have not explicitly agreed to disclose on record. This forms invisible surveillance wherein an individual can be computationally convicted or unworthy without any knowledge of it, the entitlement to any form of correction of this, and procedural equity is without any procedural fairness. The system is also likely to identify with intimately personal signs long since it exceeds acceptable cybercrime control functionality: mental health intelligence; emotional weaknesses and uses; politico-interest profiling. The other profound problem is that of algorithmic bias. The predictive models are trained in the information given to them and when this information is distributed in unrepresentative ways, such as giving a disproportionate input in respect to particular groups or behaviours, then the innocent activity-so similar to that of crime undergoes criminalisation by the AI.

Users of privacy, cybersecurity students who use exploits tools as a part of their studies, a journalist in need of anonymity to keep their sources a secret or a cyber-activist; all of them can be largely labelled as high risk largely because their statistical profile fits that of a cyber-offender. Therefore, it is structurally biased on the conversion of any predictive systems into discriminatory philtres that makes misclassification more prominent and, ultimately, results in mistrust. (Kerr 2018; OHCHR 2021) To that list include the issue of false positives. In the realm of probabilities where predictive AI functions and not certainties, even the most legitimate activity, say a student running sqlmap as a part of a penetration testing workshop or someone iterating with artistic deepfake GAN models will be identified as an offender-in-waiting. This may result in completely unjustified surveillance of their systems, to detrimental reputation and undue escalation to an investigation against them. This is further exacerbated by the fact that we do not know a lot about the reason behind AI decision making. The majority of the highest performers in transformer-based or deep learning models are also unexplainable. This renders it hard to be audited by any oversight body on the foundation of suspicion and flagged people to dispute algorithmic assumption. (Tufekci 2015) As such, robust governance regulations should be applied in which such a programme operates. These involve transparency and independent audits in the proportions of least amount of data with human-decision making within the loop of important thresholds. Otherwise, it soon transforms into a machine of action potential panoptic on policing not just the real conduct but allegedly possible wrongs of conduct directed against the basic rights and civil freedoms. (Pasquale 2015, OHCHR 2021) The true Digital Stop-and-Frisk (DSF) to cybersecurity is mostly a two-sided programme: one, being the proactive crime protection and the extremely effortless prospects of excessive enforcement in a loss of civil liberties. It would then be technological innovation in the context of cyber security as it adopts behavioural analytics; however, there are colossal setbacks in its implementation as it would demand monumental intrusion into the personal privacy to track at an exceedingly directive level all the online proceedings. This monitoring is likely to be performed without any explicit

permission by users to any manner or extent of monitoring that will ultimately not be only visually pervasive, but also an invisible-pervasive surveillance. Soon enough, this fact might evolve into an ugly dystopian DSF where people are profiled by an algorithm and labelled as a threat due to micro-behaviours that have virtually nothing to do with actual criminal intent. This would imply large scale infringements on the fundamental right to digital privacy- personal control of the virtual space. Added to all this, there is one dependency that has been introduced to DSF: dependency on the smartness of the AI models today or in any future developments and upgrades. The current systems demonstrate potential but no system will, ever, be perfect because, at the very base of it all at the very bottom of the deepest in the furthest place beyond our view as humans who now and have also created its models, every model, regardless of its training data quality, will rely entirely wholly solely completely utterly without exception whatsoever upon training data quality (!) Should there be any probability however remote improbable unlikely datasets possibly could conceivably perhaps maybe someday somewhere someway somehow again(?) be biased then, yes definitely surely positively ought to be sure will 100 percent. Will have false positives or not; or only the positives. To give an example, a student of cybersecurity who was in the process of penetration testing with the aid of the tools, or a journalist who relied only slightly more securely than the standard to the tools of communication suddenly and without any rightful cause flagged him or her as behaving suspiciously and thus disturbed his or her work with unjustified suspicion on them. Such discrimination leads to unnecessary surveillance at the same time exposing itself to the danger of reaffirming the discriminatory patterns therefore, further endangering contact of suspicion towards the system itself and the institutions that run it. Hence, the absence of transparency and explainability in AI decision making further complicates the successful realisation of DSF, since most of the most performant AI tools of today, and especially the ones founded on deep learning, are considerably black-box with minimal or no insight on how they arrive at any conclusions whatsoever. This renders it hard to challenge the decisions of their security systems by individuals evident to be unaccountable surveillance hardware

without explicit supervision. DSF may establish a popular institution over and above the democratic institutions. It is possible that there are no clear governance structures. This as such leads to a question regarding the due process and redress wherein algorithmic judgement has adverse effects on the lives of people: a debate on power abuse-governance by algorithms. The other large pragmatic issue is that of data size; very large amounts of data must be operated in real time to analyse behaviour of what could be millions of interactions between two individuals that would need a large amount of computing infrastructure. The scalability is a potential issue in the future as this technology advances since to install such high end advanced systems becomes difficult to have a smaller institution possessing enough resources to implement the efficacies when someday however criminals dynamically continuously switch to new ways of hiding their tracks when AI models constantly retrain catch up emerging tactics tools are both times consuming resource-intensive. Digital Stop-and-Frisk will be an effective instrument in preventing the occurrence of cybercrime through good governance and transparency, with the human-in-the-loop oversight. Accommodative implementation of DSF must be able to walk the thin line between the principle of individual rights and provision of security. Nonetheless, without any robust regulation frameworks that mitigate its dangers - privacy intrusions, algorithmic bias and even opacities; its application can likely see far-reaching consequences largely harmful to trust and integrity in precisely the digital settings; it is intended to safeguard by creating it. Thus, any possible success to it cannot be narrowed down to issues to do with techno-logical competence but must also be burdened with the necessity of the creation of appropriate legal/ethical frame-works within which to operate that DSF becomes not an agent of the unrelenting impetus to do what is 'good' but instead a means of creating a means of more and more destructive surveillance.

6. Conclusion:

Digital stop-and-frisk is a potent conceptualisation of the digitalized concept of policing as one that is not a response to, but a predictive functioning of, a crime. Digital interactions pick a very small signal and

much larger composite signals are constructed by next-generation AI architectures. The opportunities of this paradigm encompass the ability to become aware of any of the nascent cyber threats before the threat has grown into a harmful act. It serves a great purpose in safeguarding potential victims and key infrastructures and complicates the usual process of organised cybercrime by blocking their operating space. (Stoddart and MacDonald, 2023) Responsible rulemaking is what dams the distinction between the statistical similarity shaped further by de facto guilty behaviour than the intrusion surveillance, digital stop-and-frisk- another AI application that pretends to be law enforcement unless regulated by responsible leadership. The challenge system that has AI policing as part of the democracy system by ensuring that the enhanced security is not at the cost of disrupting the infrastructure that digital rights have been built on. When cautiously handled and ethically applied, predictive micro-targeting can be a maximally fine instrument of strategic use in cyber defence thereby increasing the already dynamically-evolutionary practise, however when unregulated it would witness the introduction of a new era of massively worrying of automated suspicion, unsteady privacy, and justice being algorithmic instead of human.

References:

1. *Liu, Y., Ji, S., Li, H., & Beyah, R. (2017). DeepLog: Anomaly detection and diagnosis from system logs through deep learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1285–1298. https://doi.org/10.1145/3133956.3134015*
2. *Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. NAACL-HLT, 4171–4186.*
3. *Brantingham, P. J., & Brantingham, P. L. (2017). Predatory crimes and the mathematics of criminal opportunities. Routledge. https://doi.org/10.4324/9781315081560*
4. *Felbo, B., Mislove, A., Sogaard, A., Rahwan, I., & Lehmann, S. (2017). Using millions of emoji occurrences to learn any-domain representations for detecting sentiment, emotion and sarcasm. EMNLP 2017 Proceedings, 1615–1625.*

5. *Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. NYU Press.*
6. *Kerr, O. S. (2018). Computer crime law (4th ed.). West Academic Publishing.*
7. *Office of the United Nations High Commissioner for Human Rights (OHCHR). (2021). The right to privacy in the digital age. https://www.ohchr.org*
8. *Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.*
9. *Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13(1), 203–218.*
10. *Stoddart, E., & MacDonald, S. (2023). Artificial intelligence, policing and the public interest: Rebalancing risk and rights. AI & Society, 38, 1381–1392. https://doi.org/10.1007/s00146-022-01587-0doi.org/10.1007/s00146-022-01587-0*

Author Profile:

Dr. Sachiv Kumar, Reader in Law in Lal Bahadur Shastri National Academy of Administration. He has done the Masters in Public Administration, LL.B., LL.M., Ph.D. (Law), served in National Company Law Tribunal Ahmedabad Bench as Joint Registrar; Rajiv Gandhi National University of Law, Punjab and Army Institute of Law as Assistant Professor. As a researcher, Dr. Sachiv has also contributed articles and research papers in Journals and has delivered Special lectures on various legal issues. Dr. Sachiv also Chaired Session in National and International Seminars, Judged Moot Court Competitions, Member National Lok Adalat, Member and Referee of National Journals (ISSN).

Mr. Lakshya Sharma serves as a Teaching Associate in Political Science and Constitutional Law at the Lal Bahadur Shastri National Academy of Administration. He holds a Bachelor of Arts (Honours) in Political Science from the University of Delhi, as well as a Master's degree in Political Science from IGNOU and a B.A.LL.B.(Honours). His academic background equips him with a robust understanding of political theories and legal frameworks, enhancing his contributions to the field of education and research in political science and law.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P. 109-125)

Rethinking Arrests in Consensual Adolescent Relationships under the POCSO Act: A case study of Tamil Nadu

Anindita Pattanayak* & Swagata Raha**

I. Introduction

The Protection of Children from Sexual Offences Act, 2012 (POCSO Act) criminalises all sexual acts involving a "child" i.e., a person under 18, irrespective of consent. Such acts constitute rape under the erstwhile Indian Penal Code 1860 (IPC), and the Bharatiya Nyaya Sanhita 2023 (BNS). While aimed at prosecuting sexual offences against children, the law also criminalises consensual sexual activity involving older adolescents.

Sentences prescribed for penetrative sexual offences are extremely high, ranging from a minimum of 10 years for penetrative sexual assault to the death penalty for aggravated cases. Repeated sexual acts with a minor, sexual acts resulting in the minor getting pregnant, and sexual acts where the accused is related to the minor by marriage attract a minimum sentence of 20 years. These offences are also classified as "heinous" under the Juvenile Justice (Care and Protection of Children) Act, 2015 (JJ Act),

*Anindita Pattanayak is Senior Legal Researcher and Swagata Raha is the Director-Research at Enfold Proactive Health Trust. *We are grateful to Shruthi Ramakrishnan from Enfold Proactive Health Trust for her support in conducting interviews and analysis.*

making it possible for adolescents above 16 engaging in consensual sexual acts to be tried as adults. In recent years, courts and civil society have raised concerns about the criminalisation of factually consensual and non-exploitative relationships involving adolescents. Empirical studies based on court judgments indicate that "romantic" cases constitute at least one-fourth of cases being decided by Special Courts, with families of victim girls being the primary informants (Enfold, 2022 & 2024, Prasad and others). Male parties in consensual relationships are routinely charged with non-bailable offences like rape or penetrative sexual assault. Though the law is gender-neutral, where both parties are minors, the boys are considered perpetrators and girls are labelled victims. Often, "victims" in such cases turn hostile, resulting in acquittals. Despite low conviction rates, many men and boys are incarcerated without bail. As per a study (Enfold Proactive Health Trust, 2022), the accused remained in judicial custody until trial concluded in 15.2% of "romantic" cases studied under POCSO Act.

Arrests severely disrupt the accused's education, employment, and future prospects, particularly for minors, in respect of whom the Juvenile Justice (Care and Protection) Act 2015 (JJ Act) upholds institutionalisation as a measure of last resort. The higher judiciary has consistently held that arrest curtails liberty, causes trauma, humiliation, and stigma to the accused and their families. Specifically, in consensual cases involving adolescents, High Courts have noted that arrest strains the relationship between the couple and their families, and acknowledged that exploring romantic relationships is a normal part of adolescent development.[1]

Noting the disproportionately adverse effect of arrest in consensual cases, the Tamil Nadu Police opted to issue a notice under Section 41A of

[1] *State of Karnataka v. Basavraj S/O Yellappa Madar, Criminal Application No. 100515 of 2021 (Karnataka High Court, 4 November 2022); Sabari v. the Inspector of Police, Criminal Appeal No.490 of 2018 (Madras High Court, 26 April 2019); Vijayalakshmi v. State, Criminal Original Petition No.232 of 2021 (Madras High Court, 27 January 2021); Pooja and Ors. v State of U.P. and Ors, Application U/S 482 No. 136 of 2016 (Allahabad High Court, 29 February 2024); Rama @ Bande Rama v. State of Karnataka, Criminal Petition No. 6214 of 2022 (Karnataka High Court, 2 August 2022*).

the Code of Criminal Procedure 1973 (CrPC) in lieu of arrest. In November 2022, the Juvenile Justice Committee and the POCSO Committee of the Madras High Court convened a State Level Consultation with stakeholders from Tamil Nadu and Puducherry, including the police on POCSO Act implementation. The police practice of issuing a Section 41A to the accused in POCSO cases involving a consensual relationship was brought to the attention of the Committee. Noting that "60% of POCSO cases that are registered relate to mutual romantic relationships", the High Court passed a resolution directing the Director General of Police (DGP) to instruct investigating officers (IOs) in POCSO cases:

> "a) not to show haste in effecting arrest of the accused in mutual romantic cases;
> b) instead issue a notice under Section 41 A Cr.P.C to the person concerned for enquiry;
> c) record in the case diary, the decision for not arresting the accused, along with the reasons therefore; and
> d) resort to arrest only with the permission of the Superintendent of Police / Deputy Commissioner of Police, as the case may be."

The operative portions of the resolution were circulated by the DGP to all Commissioners and Superintendents of Police in a State-wide circular dated 3 December 2022, followed by another explanatory circular in Tamil dated 30 April 2023 ("the Circular").

While the POCSO Act does not recognise the possibility of consent, this article explores the Tamil Nadu Model of using Section 41A, CrPC/Section 35, Bharatiya Nagarik Suraksha Sanhita (BNSS) in "mutually consensual" adolescent POCSO cases.

Methodology:

Interviews were conducted with police officers in Tamil Nadu between August and September 2024, including an Additional Commissioner of Police, a Deputy Commissioner of Police in Chennai, an inspector and two sub-inspectors in Chennai, and two Superintendents of Police from Theni and Madurai. Three defence counsel (including one who exclusively

practices before the Juvenile Justice Board in Chennai), a public prosecutor in Chennai, and a civil society organisation (CSO) working closely with victims and children in conflict with the law in POCSO cases in Chennai) were interviewed. Dr. Mrinal Satish, Professor and Dean (Research) at the National Law School of India University, Bangalore, and an expert on criminal law, was also interviewed. Relevant Madras High Court decisions and the legal framework on Section 41A CrPC were examined.

Based on a limited set of interviews, this article is exploratory in nature and not a comprehensive study. It aims to capture early patterns, challenges and key themes that merit further study and highlight a current police response to the harms of over-criminalisation in such cases.

Legal Framework:

Section 41(1), CrPC/Section 35(1), BNSS states grounds on which a police officer may arrest in a cognizable offence. The Supreme Court has repeatedly held that the power of arrest is discretionary and should be used judiciously.[2] In *M.C. Abraham and Ors. v State of Maharashtra*,[3] it observed that,

> "[police] is not expected to act in a mechanical manner and in all cases to arrest the accused as soon as the report is lodged. In appropriate cases, after some investigation, the investigating officer may make up his mind as to whether it is necessary to arrest the accused person…. **Since the power is discretionary, a police officer is not always bound to arrest an accused even if the allegation against him is of having committed a cognizable offence.** Since an arrest is in the nature of an encroachment on the liberty of the subject and does affect the reputation and status of the citizen, the **power has to be cautiously exercised.**"

[2] *Arnesh Kumar v. State of Bihar, (2014) 3 SCC (Cri) 449; Satendar Kumar Antil v. Central Bureau of Investigation (2022) 10 SCC 51; Mohammed Zubair v. State of NCT of Delhi, 2022 SCC OnLine SC 897.*

[3] *2003 (2) SCC 649. See also Acharya Bal Krishna v. C.B.I., Criminal Miscellaneous Application No. 1252 of 2016 (High Court of Uttarakhand, 16 July 2018).*

Earlier, the Supreme Court in the case of *Joginder Kumar v State of Uttar Pradesh*[4] had emphasised that

> "No arrest can be made because it is lawful for the police officer to do so. The existence of the power to arrest is one thing. The justification for the exercise of it is quite another…. Except in heinous offences, an arrest must be avoided if a police officer issues notice to person to attend the Station House and not to leave the Station without permission would do."[5]

The Supreme Court thus delineated the process of issuing a notice instead of making an arrest. However, it envisaged this process for non-heinous offences. It outlined justifiable reasons to arrest based on the third report of the National Police Commission which included the likelihood of the accused absconding and restraining the accused to infuse confidence among victims of grave offences such as murder, dacoity, robbery and rape.[6]

Referring to *Joginder Kumar*, the Law Commission of India in its 152nd Report on Custodial Crimes (1994) recommended the insertion of Section 41A to enable a police officer to issue a notice of appearance to the

---

[4] *AIR 1994 SC 1349.*

[5] *Joginder Kumar v. State of Uttar Pradesh, AIR 1994 SC 1349, para 20.*

[6] *National Police Commission, Third Report of the National Police Commission (1980), para 22.28, available at https://police.py.gov.in/Police%20Commission%20reports/3rd%20Police%20Commission%20report.pdf; See also Law Commission of India, 152nd Report on Custodial Crimes (1994), para 14.4, available at https://cdnbbsr.s3waas.gov.in/s3ca0daec69b5adc880fb464895726dbdf/uploads/2022/08/2022080893-2.pdf - "the recommendation of the Law Commission of India in its 152nd Report in 1994 recommended the insertion of a new section on arrest in respect of cognizable offences providing that a police officer arresting a person should be reasonably satisfied as to the person's complicity in the commission of the offence and that "arrest is necessary in order to bring the movements of the person arrested under restraint, so as to inspire a sense of security in the public or to prevent the person to be arrested from evading the process of the law or to prevent him from committing similar offences or from indulging in violent behaviour in general."*

accused in a cognisable offence instead of arresting them.[7] This was reiterated by the Law Commission of India in its 177th Report on the Law of Arrest (2001) where it was recommended that the police officer may "in all cases where the arrest of a person is not required under the provisions of Section 41, issue a notice directing the person against whom credible information has been received that he has committed a cognizable offence, to appear before him or the court, as the case may be, whenever called upon to do so." While advising against arrest in most offences punishable with less than seven years, the 177th Report also suggested that

> "In the case of serious offences… punishable with imprisonment exceeding seven years, arrest may be called for instilling a sense of confidence among the members of the public."

Ultimately, Section 41A of the CrPC was introduced in 2008, giving the police an option to issue a notice of appearance in lieu of arrest regardless of whether the offence is heinous. Due to concerns regarding misuse, an amendment in 2010 to the Section made it mandatory for police to issue such notices when deciding not to arrest. This provision is now replicated in Section 35(3)-(6) of the Bharatiya Nagarik Suraksha Sanhita 2023 (BNSS). Section 41A, Cr.P.C/Section 35(3), BNSS provides that in cases where arrest is not deemed necessary, the police officer must issue a notice of appearance to the person against whom a reasonable complaint, credible information, or reasonable suspicion exists regarding the commission of a cognizable offence. The individual must appear as directed, and if they comply, they cannot be arrested unless reasons are recorded. Non-compliance may result in arrest, subject to court orders.

More recently, in *Arnesh Kumar v. State of Bihar*,[8] the apex court urged reflection on the purpose of arrest, observing that

---

[7] *Law Commission of India, 152nd Report on Custodial Crimes (1994), paras 5.7-5.10, 14.6, available at https://cdnbbsr.s3waas.gov.in/s3ca0daec69b5adc880fb464895726dbdf/uploads/2022/08/2022080893-2.pdf.*

[8] *(2014) 3 SCC (Cri) 449.*

> "the police officer before arrest must put a question to himself, why arrest? Is it really required? What purpose it will serve? What object it will achieve?"

While *Arnesh Kumar* encouraged the use of Section 41A, Cr.P.C in offences punishable with less than seven years, it did not delve into the application of the provision in cases of offences with more than seven years imprisonment. The Andhra Pradesh High Court in *Meka Sai Nagendra v. State of Andhra Pradesh*[9] interpreted *Arnesh Kumar* to mean that Section 41A applies only to offences punishable with less than seven years. It should, however, be noted that this decision is applicable only to Andhra Pradesh. Notably, the text of Section 41A, Cr.P.C does not limit its scope to offences based on the severity of punishment and applies to all cognizable offences.

The Tamil Nadu Model:

The Tamil Nadu model reflects the qualified use of Section 41A, Cr.P.C in offences under the POCSO Act involving mutual romantic relationships. Through the Circular, it aims to mitigate the adverse impact of arrest on the accused person's life, dignity, and livelihood, and minimise harassment and stigmatisation. It also seeks to alleviate the hardship on the victim and families of the couple, especially from financially vulnerable backgrounds. It acknowledges that many mutual romantic POCSO cases result in the victim turning hostile and ultimately lead to acquittals, burdening the criminal justice system unnecessarily.

Interviews with police officers, defence counsel, a public prosecutor, and a CSO revealed that the Circular is being actively implemented in the State. Three senior police officials, who were all interviewed in the preparation of this article documented the use of Section 41A in consensual relationships attracting POCSO charges in the districts of Kanyakumari, Madurai and Theni in a previous issue of this journal (Prasad *et al*, 2023). They noted that in these districts, 74% of the registered POCSO cases were of "mutual consensual relationship/love affair/elopement." They outlined the following procedure followed in cases where notice under Section 41A were issued instead of arrest:

---

[9] *2024 SCC OnLine AP 2239.*

1. "Notice u/s. 41 Cr.P.C was served and the reasons for not effecting arrest were recorded in the Case Diary.
2. The decisions of not effecting arrest were taken on a case-by-case basis by following due diligence by the supervisory Officers by taking into account, the social, economic and educational background of the families, the medical condition of the child involved and other relevant factors.
3. The so-called accused were informed not to apply for bail since applying for bail would nullify the very purpose for which the decision was taken not to effect an arrest.
4. Investigating Officers would record the statements and collect evidences as it is without any fear and ignorance."

Recording Reasons Not to Arrest:

With a view to ensure that the discretion is not unchecked, **the Circular requires reasons for not arresting the accused to be recorded, although the CrPC/BNSS does not require this**. Before the 2010 amendment, Section 41 required police officers to record reasons for arrest in cognizable offences punishable with imprisonment of less than seven years. The 2010 amendment introduced an additional requirement for police officers to record reasons for not making an arrest in such offences. Discussions in the Lok Sabha during the passage of the 2010 amendment highlight that both measures – recording reasons to arrest and not to arrest in the case of cognisable offences attracting less than seven years punishment – were intended to prevent arbitrariness in police action. These discussions reveal a significant concern regarding the potential for police officers to misuse their discretion by choosing not to arrest, driven by apathy, dereliction of duty, or collusion with influential individuals especially in offences against women that attracted punishment of less than seven years of imprisonment. The assumption while passing this amendment was that offences punishable with imprisonment of more than seven years would invariably result in arrests, making it unnecessary to mandate the recording of reasons for not arresting in such cases. However, as the provision currently stands, Section 41A can be applied in all

cognizable offences, regardless of the severity of the punishment. Yet, **the requirement to record reasons for not arresting the accused applies only to offences punishable with imprisonment of less than seven years. This discrepancy raises concerns about the potential corruption and misuse of police power. Thus, the additional requirement to record reasons for not arresting introduced by the Circular is a crucial safeguard against such risk.**

From the interviews, it appeared that the actual implementation of this requirement varied on the ground. One officer shared that there is no need to record reasons as the police power to arrest is entirely discretionary. However, in districts like Theni, reasons for not arresting the accused are recorded by the IO in the case diary. The reason usually recorded is that the relationship appears mutually consensual and that the accused is willing to cooperate with the police investigation by appearing at the station when summoned.

It also appeared that the decision of IOs to issue a 41A notice is closely supervised by their superiors. A supervisory officer and IO independently shared that, the former reviews the relevant details of the consensual cases under POCSO during the Daily Situation Report (DSR), checks if the IO has taken the statement of the medical officer, the parents of the victim etc., and works with the IO to arrive at a conclusion about whether an arrest is necessary or a notice under Section 41A should be issued. A senior officer in Chennai, who undertakes these supervisory functions on a daily basis, emphasised that they trust the judgment of the IOs noting that decisions largely depend on the ground level officers' assessment of the facts and their understanding of the case. In Theni, the IOs are encouraged to call the supervising officer when they receive a consensual case under POCSO, to discuss whether to issue a 41A notice.

Ascertaining Consent:

The police interviews provided insight on the manner in which mutual consent is ascertained. A woman IO talks to the victim to understand whether there was a romantic relationship between her and the accused. Heavy reliance is placed on the victim's statement to the police to arrive at

a conclusion. Significant emphasis is placed on whether the victim herself states that she consented to the sexual activity or was in a relationship with the accused. Some IOs shared that on talking to the victim, her family, and school friends, it becomes obvious whether it is a "true" POCSO case or a romantic relationship. They also consider what the victim states during the medical examination to the medical officer. For instance, one officer shared that the victim sometimes reveals to the medical officer that she consented to sexual intercourse or that the accused was her boyfriend.

The following factors emerged that were not articulated in the Circular but appear to be followed while implementing the Circular:

1. **Application in cases of victims above 16 years:** Although the Circular does not prescribe any age threshold, interviews revealed that the notice under Section 41A is issued in consensual cases where the victim is very close to the age of majority, typically 17 years old. Some officers prefer not to apply the Circular to cases where the victim is below 16 years old. Nonetheless, there have been instances where the Circular has been applied even when the victim is 14-15 years old.
2. **Consideration of statement to Magistrate under Section 164, Cr.PC:** Three senior officers, one inspector and the public prosecutor shared that as a precautionary measure in some cases where they are unsure, a Section 41A notice is issued only after the victim's statement is recorded by a Magistrate under Section 164 of the CrPC/Section 183 of BNSS. If the victim does not implicate the accused in her statement and alludes to it being a consensual relationship, the notice is issued.
3. **Consideration of aggravating factors:** Some respondents shared that arrest is preferred over issuing a Section 41A notice if there are aggravating factors such as the victim experiencing repeated pregnancies, allegations of physical violence, or a significant age gap between the victim and the accused. An officer gave an example where the accused was already married and around 35-years-old

while the girl was 17 years, explaining that arrest is considered more appropriate in such a case.

4. **Consideration of mitigating factors:** Conversely, some respondents shared that a Section 41A notice is considered when the victim and accused are close in age, living together as a couple, are married, or when the victim is pregnant with the accused's child within the context of the marriage.
5. **Views of the family:** While a sub-inspector shared that a Section 41A notice is not preferred if the family of the victim insists it is non-consensual case, other officers shared that the opinion of the victim's family or the pressure exerted by them is not a factor considered in deciding whether to issue a notice under Section 41A. They acknowledged that families often disagree with the girl's account, particularly in inter-caste or inter-faith relationships, but emphasised that they explain the legal position to the parents and proceed based on their own assessment rather than yielding to pressure from the family.
6. **Supervision:** Officers shared that the decision of the IO about whether to arrest or issue a Section 41 A notice is supervised by senior officials so as to ensure that there is internal oversight and arbitrariness is kept in check.
7. **Safety of the accused:** Two of the officers interviewed also shared that they consider making an arrest if it appears that local hostile elements pose a threat to the accused or there is a likelihood of law and order issues due to communal or caste differences.

A recurring theme across interviews was the idea of a "genuine" romance, sometimes contrasted with a mere infatuation. Lawyers and officers recognised the idea of teen relationships and young love, typically within the same age group, some describing them as "innocent". However, deviations from this conception—such as when the boy refused to marry the girl after intercourse, was already married or had children with another woman—were deemed exploitative and not considered fit cases for a Section 41A notice. The factors used to distinguish "genuine" love from exploitation were highly subjective and varied widely. For example, one

sub-inspector viewed the deliberate planning of sexual activity, such as booking a lodge in advance, as evidence of a nefarious mindset. She also cited repeated pregnancies as signs of continued exploitation. In contrast, another officer described a case where a Section 41A notice was issued because the girl had eloped, married the accused, and was pregnant with his child—circumstances seen as reflecting innocent romance.

While it is difficult to draw conclusions with any certainty, it appears that a relationship is considered "consensual" not merely when the sexual act is voluntary, but when it aligns with the officer's notion of an "innocent" relationship.

Perceived Benefits of the Circular:

All respondents agreed that the Circular is a welcome intervention that prevents unnecessary stigmatisation and trauma and allows for a sensitive approach to the case while the trial continues. Some added that the POCSO Act was not meant to address consensual cases. Nearly all the respondents mentioned that these types of cases often result in an acquittal and that the primary hardship suffered by the accused is in the process of arrest, investigation and trial. An officer shared that

> "it is definitely helping by preventing kids from being stigmatised as a criminal for being in a romantic relationship. With this, they can continue education and be with their parents instead of going to an Observation Home [If there is apprehension] there is also an economic pinch on poor families to catch an advocate for bail, that also takes an economic cost. Not every family can afford a good lawyer."

According to the respondents, the Circular also eases operational burden. Police officers noted that they are often overburdened with additional duties related to law and order and security, and POCSO cases involve time-consuming steps such as medical examinations and discreet house visits in plain clothes and unmarked vehicles. In this context, eliminating the requirement for arrest reduces their workload. However, the public prosecutor interviewed shared that although no arrest is planned, many accused still file anticipatory bail petitions especially when the police often wait until the victim's Section 164 statement is recorded before

making a final decision. This leaves the accused anxious, and compels the prosecution to oppose bail despite no immediate intention to arrest.

Concerns about the Implementation of the Circular:

The absence of guiding principles to ascertain "mutually romantic" cases raises concerns regarding arbitrariness in the application of the Circular. One Inspector explained that officers are encouraged to issue Section 41A notices whenever possible and described a case involving allegations of physical violence where she was advised to issue a Section 41A notice instead of arrest, as the victim and accused were likely to continue their relationship. In contrast, other officers preferred arrest in similar cases, particularly where the accused was violent with the victim. These variations show how similar cases are treated differently based on the officer's discretion, local context, and subjective assessments of consent and exploitation.

The CSO respondent shared that cases involving grooming, the girl being pressured to state there is a mutually consensual relationship, or sexual assault within romantic relationships are complex and require skills to ascertain the presence of exploitative elements. Concerns were also raised about corruption, citing cases where police accepted money from the accused and framed non-arrest as a favour.

There is also a risk that powerful individuals could influence the police to avoid arrests, effectively silencing victims and undermining the purpose of the law. One police officer interviewed also shared that men no longer fear the law now that arrest is not the default action taken.

Conclusion:

Blanket criminalisation of adolescent sexuality has resulted in the unfair disruption of adolescent lives and stretched limited state resources. In July 2023, the Madras High Court drew attention to the burden such cases place on the criminal justice system and directed the DGP to identify and segregate the consensual cases amongst the POCSO cases pending before the Juvenile Justice Board so that the High Court can "quash the

proceedings if the proceedings are ultimately going to be against the interest and future of the children involved in those cases."[10]

In this context, the Tamil Nadu Model is an innovative approach to address one aspect of the criminalization of normative adolescent sexuality, focusing on alleviating the trauma, deprivation of liberty, and humiliation associated with arrests in consensual cases under the POCSO Act. By leveraging existing legal provisions, the model attempts to mitigate the immediate harms caused by arrests. Stakeholders implementing the model perceive significant benefits in reducing hardships for both the accused and the alleged victim in such cases with the police also finding it helpful in reducing the burden on the criminal justice system.

Its adoption has been facilitated by **collaborative efforts between the judiciary and police**, preceded by stakeholder consultations, fostering a common understanding of the issue within the system. Nonetheless, since the police power to arrest is discretionary, officers may adopt a policy of issuing notices instead of making arrests without any judicial intervention, as was the case in Tamil Nadu prior to the issuance of the Circular. Though arrest is avoided, the criminal trial proceeds as usual, and questions of justice and accountability are addressed during the judicial process. **The accused does not face reduced culpability or escape the consequences of their alleged actions merely because a Section 41A notice was issued instead of an arrest**.

However, the model faces challenges. A key concern is the potential for arbitrary police action due to the absence of clear guidelines on ascertaining "mutual consensual" relationships. Decisions about whether a case qualifies as consensual are often informed by subjective interpretations of societal norms on what is an acceptable romantic or sexual relationship, which can vary widely. Limitations also include challenges in the identification of exploitative elements in such relationships. Additionally, there is a risk of motivated decisions, in cases involving powerful individuals, undue inducements or caste-based,

[10] *Kajendran v. Superintendent of Police, Habeas Corpus Petition No.2182 of 2022 (Madras High Court, 7 July 2023).*

religious or other social factors, which may result in discriminatory application of the provision.

To address these concerns, the requirement in the Circular for the police to record reasons why the accused was not arrested should be strictly adhered to, including reasons in the best interest of the child concerned, coupled with regular supervisory oversight. This will reduce the potential for arbitrariness and ensure application of mind in determining whether to arrest. Further, a guiding framework may need to be developed to identify consensual cases and reduce bias. Determination of a minimum age below which Section 41A notices would not apply or establishing an acceptable age difference between the victim and the accused may be considered. The guiding principles could also outline whose statements are critical and the factors to consider when determining consent. Furthermore, they should account for scenarios where arrest is necessary despite claims of a consensual relationship, such as when there is evidence of violence, exploitation, trafficking or the safety of the accused or the victim cannot be assured due to tensions within the community in the aftermath of the incident.

Additionally, the issue of notices, though informed by the experience of the officers on the ground, should be well-supervised and data regarding arrests and issue of notices should be maintained in an organised way for accountability, monitoring and research. Regular monitoring of cases, detailed recording of reasons for arrest or non-arrest in case diaries, and periodic consultations with stakeholders to update the guidelines based on the experiences of implementing the model would further enhance consistency and reduce the scope for arbitrariness.

The Tamil Nadu Model offers a promising approach to balancing the need for justice with the protection of individual rights. Further research is required to analyse the long-term impact of the model, and identify evidence-based areas for improvement.

By addressing concerns of arbitrariness and ensuring consistent application, the Tamil Nadu Model could serve as a blueprint for other jurisdictions to reduce harm in cases involving adolescent relationships.

References

1. *Tamil Nadu Police, Circular memorandum, Rc.No.009464/Crime-4(3)/2022 dated 3 December 2022.*
2. *Enfold Proactive Health Trust, UNFPA & UNICEF. (2022). Implication of the POCSO Act in India on Adolescent Sexuality: A Policy Brief. Retrieved from https://www.girlsnotbrides.org/documents/1960/POSCO-Act-Policy-Brief_wUlR95W.pdf .*
3. *Enfold Proactive Health Trust. (2022). "Romantic" Cases under the POCSO Act ("Enfold 2022"). Retrieved from https://www.girlsnotbrides.org/documents/1951/Romantic-cases-under-the-POCSO-Act_wUNsbKC.pdf*
4. *Enfold Proactive Health Trust, P39A. (2024). The Verdict and Beyond: Judicial trends and Survivor narratives in child sexual abuse cases, Retrieved from https://www.project39a.com/the-verdict-and-beyond-report*
5. *Prasad, R.S., Dongare, P. and Prasad, H.K. (2023). Insights into POCSO Cases Investigation: Twin Approach Addressing Societal Realities and Legalities: Tamil Nadu Model. Sardar Vallabhbhai Patel National Police Academy Journal, LXII(1), 184-200. Retrieved from https://www.svpnpa.gov.in/static/gallery/docs/ea70ec35f79946e999264ed4a08c565b.pdf ("Prasad et al, 2023").*
6. *Ramaseshan, G. (2012). Control & Freedom: Women & The Age of Sexual Decisions.*
7. *CCL-NLSIU. (2017). Study on the Working of Special Courts under the POCSO Act, 2012 in Maharashtra.*
8. *National Police Commission. (1980). Third Report of the National Police Commission.*
9. *Law Commission of India. (1994). 152nd Report on Custodial Crimes.*
10. *Law Commission of India. (2001). 177th Report on Law Relating to Arrest.*
11. *Law Commission of India. (2023). 283th Report on Age of Consent under Protection of Children from Sexual Offenses Act 2012.*
12. *Rajya Sabha Discussion. (18 December 2008). Session 214. Discussion on The Code of Criminal Procedure (Amendment) Bill, 2008.*
13. *Lok Sabha Discussion. (12 August 2010). Session V on the Code of Criminal Procedure (Amendment) Bill, 2010.*
14. *Juvenile Justice Committee of Madras High Court. Circular memorandum, Rc.No.009464/Crime-4(3)/2022 dated 3 December 2022.*

Author's Profile
Anindita Pattanayak is Senior Legal Researcher and Swagata Raha is the Director-Research at Enfold Proactive Health Trust. We are grateful to Shruthi Ramakrishnan from Enfold Proactive Health Trust for her support in conducting interviews and analysis.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P. 126-143)

Evolving Nature of Transnational Organized Crime in India: Need for Rethinking Counter Policing Strategies

Parvesh Shaikh*

Abstract:

The Organized crime since the 1980s has shifted from local and national to an international facet that transcends national borders, termed Transnational Organized Crime (TOC). The criminal syndicates constantly evolve their operations and modus operandi, exploiting new technologies and opportunities. This paper examines the evolving nature of TOC in India, highlighting sophistication in their approach by integration of digital technologies like use of drones, dead drops in drugs, use of encrypted platforms, and cryptocurrencies, ensure anonymity in operations; in arms trafficking, cyber slavery, and drug smuggling rackets. Through case analyses from open access news media, including Delhi Police's bust of a Pakistan-linked arms racket and Gujarat Police's disruption of cyber slavery networks. The paper proposes advanced counter policing strategies such as AI- driven link analysis, anti-drone systems, and capacity building in cyber forensics to redefine policing approach towards fight against tech-savvy organized criminal syndicates.

Keywords:

Transnational Organized Crime, Digital Tradecraft, Cyber Slavery, AI, Policing.

* *Deputy Assistant Director (Lecturer), North Eastern Police Academy, Ministry of Home Affairs, Government of India*

1. introduction:

Crime in India has evolved from ancient religious and community-based justice (Dharmashastra) to Islamic jurisprudence (Medieval period) and then a formalized, pre modern colonial system with the enactment and execution of the Indian Penal Code (1860), which created new crime categories of offences. Post-independence, modernization, urbanization, and economic reforms in India brought about by 1991 Liberalisation, Privatisation, and Globalisation (LPG) led to systemic and social changes in the country followed by new drivers like consumerism, open market, industrialization, increase in population and migration to urban hubs all contributing to an uptick in crime and changes in trends and patterns of crimes such as increase in violent crimes linked with various internal security and national security threats notably Terrorism, Insurgency, Naxalism and Separatism. In the people's domain certain crimes specifically crime against women and children, juvenile delinquency, financial crimes and white collar crimes and with the advancements of technology and internet in the early 1999s the new forms of cyber crimes from simple phishing, smishing, financial fraud, identity frauds, hacking to most sophisticated cyber crime primarily cyber enabled harassment of women & children, cyber extortion, cyber terrorism and cyber enabled organized crimes are the emerging threats of the day. These crimes leave footprints on the digital space causing harms and effects in the physical spaces. The most past, present & future to the centre of all criminal activities happens to be organized crime.

Organized crime in India has seen new phases from time to time. The bandits, pindaris, thugs and pirates spread their terror on land and in the seas. To the more evolving nature of organized crime shifting its footprint beyond borders and taking the shape of transnational organized crime.

1.1 Organized vs Transnational Crime: The Planned Criminal Behaviour

Organized crime refers to highly centralized criminal networks operated by individuals or groups for the purpose of engaging in illegal activities, often with significant social, economic, and political consequences. Organized

crime involves a structured hierarchy, long-term planning, and coordination among the networks that are connected like tentacles that spread across various sectors of society.

These "tentacles" extend beyond direct criminal acts to infiltrate and destabilize legal systems, economies, and politics globally.

1.2 The Structure:

Organized crime shadows a legal organization to sustain its activities in terms of right man for the right job, chain of command, focus on profits and gains at any cost, skilling the ground force with techniques of committing crimes. The criminal network adopts planned and systematic executions of illegal activities with a proper administration and links in place.

Traditional Organized crime which incorporates illicit liquor, kidnapping, prostitution rackets, gambling, betting, blackmailing, trade extortion, sand mafia, contract killing, mining mafia, pornography and many other, the second type is non-traditional organized crimes which consist of transnational crimes human trafficking, cybercrime, money laundering, arms smuggling, pumping fake Indian currency, hacking, drug smuggling etc.

Organized crime takes many forms, one of the most modern is Transnational Organized Crime (TOC). Organized crime since the 1980s has shifted from local and national to an international frame that transcends national borders into a foreign territory, what is commonly termed as the Transnational organized crime. It is constantly evolving, exploiting new technologies and opportunities. The criminal gangs or syndicates operate on an international scale with advanced coordination and networking, eyeing for lucrative markets for illegal goods and services. The gangs take advantage of cross border mobility and exploit vulnerable points to evade prosecution. Much of the illegal goods and services that are smuggled across borders are prohibited or highly taxed goods like child pornography, stolen motor vehicles, pirated textiles, counterfeit medicines & currency, protected wildlife items, cultural artifacts, arms, drugs, technology,

hazardous waste, gasoline, liquor, cigarettes etc, (Kleemans & De Poot, 2008).

The present research paper highlights key transnational and national organized criminal activities of the day and their evolving modus operandi and sophistication utilizing private digital spaces in commission of trafficking and smuggling thus an intersection of physical and digital space is the new landscape of organized crime that demands redefining policing strategies in countering new age crimes with proper security infrastructure in place.

1.3 Objectives of the Study:

- To trace the shift from traditional to transnational organized crime in India, focusing on technology-enabled operations.
- To analyze recent case studies revealing common digital tactics like dead drops, encrypted communications, and cross-border drone deliveries.
- To suggest counter policing strategies, including use of AI tools, behavioral analytics, and forensic enhancements for disrupting criminal networks.

1.4 Methodology and Data Sources:

The analysis relies on secondary data from open-access media reports, government statements (e.g., Rajya Sabha responses on cyber slavery rescues), UNODC publications, findings of official reports like the Narcotics Control Bureau Annual Report 2024 and DRI Smuggling Report 2024-25, and case-specific investigations by Delhi Police, Gujarat Police CCoE, and NCB Chennai Zone.

2. The Evolving Nature of Transnational Organized Crime: Recent Case Scenarios

Since the mid-1980s, profound changes and advances in technologies have driven the emergence of a digital society (Dufva, 2019). The technologically fuelled revolution, the instance of birth of the Internet, the World Wide Web, increase in the number of electronic computers, including personal computers, gadgets have connected to the Internet with

unstoppable speed and that has become the integral part of human lives. This digitally connected society also has a strong impact on the world of crime. Crimes are changing, in terms of typologies and modus operandi. Every now and then criminals change, their characteristics, their social interactions, and their relationships with potential victims (Di Nicola, 2022). Where there are new social facts, new habits, new ways to meet, buy, pay, save, protect, transfer assets, new digital identities, new systems for information gathering, self-organization, pleasure, and travel, it is only natural that new crimes and new ways to fight crime also emerge. And this is especially true for organized crime, which is committed by organized criminal collectivises that, according to the principles of rationality, always seek to take advantage of new opportunities, maximize their profits, and minimize the risks.

In the recent past organized criminal gangs have evolved their modus operandi by imbibing technology in their daily operational planning, moving beyond traditional violence and territory to effectively use the Internet for global reach, anonymity, and expanding new crimes like cyber fraud, using tools such as dark web markets for illicit goods, cryptocurrencies for money laundering, remote drones technology for cross border smuggling and AI/deepfakes for complex financial manipulation and disinformation. The easy access to the Internet era has influenced various criminal economies, from drug trafficking to money laundering. In Mexico, for example, producers of synthetic drugs, such as fentanyl and methamphetamine, use the open and dark web to acquire precursors and highly regulated chemicals through sellers who can ensure successful shipments to almost anywhere.

The Cases:

I. Transnational Arms Trafficking Racket:

According to UNODC arms trafficking involves cross-border transfers of firearms, their parts, components, or ammunition that are unauthorized by at least one of the countries involved, or which lack proper identification or markings. The arms trafficked cross border fuels, crimes, violence, terror, and bloodshed. Arms trafficking is important for the activities of organized

criminal groups, from local street gangs to cartels operating across borders to survive their activities and commit serious crimes, gain power, and maintain control, instil fear, challenge authority, and undermine the rule of law.

Illegal weapons have high market value, and traffickers profit significantly from their sale.

The Case: Recently in November 2025 the Delhi Police cracked an International Arms Trafficking racket that was supplying weapons made in China and Turkey to Organized Criminal Groups in North India with locally based handlers in Punjab. The syndicate was suspected to be linked with Pakistan's Inter-Services Intelligence (ISI). In this operation the police recovered 10 expensive foreign made pistols (China made PX-3 pistol and Turkey made PX-5.7 pistol) and 80 to 90 live cartridges.

Evolving Modus Operandi: Based on the initial investigation it was found that the consignments of pistols wrapped in carbon paper were dropped using drones at designated locations or vulnerable points close to the border at pre-selected GPS locations during night time.

Key Operational Planning & Execution: The drones were flown at low altitude and the consignments packed in carbon paper solely for they did not get detected easily and to escape the radar. The supply was dropped in small but high value payloads. The drop locations and time were frequently changed to avoid any similar pattern and to deceive border guarding forces.

Advanced Digital Tradecraft: The criminal gang was communicating with the regional sub agents' cross border through encrypted communication platforms. This facilitates seamless anonymous coordination and hide the identity and plans.

II. Transnational Cyber Slavery Racket:

Cyber Slavery is the modern-day digital trap a technologically assisted human trafficking, an intersection of human trafficking and digital exploitation. In this act humans especially the qualified youngsters both males and females in the search jobs are trapped and lured with fake attractive job offers with lucrative salaries and package through social

media and other online media. The victims are trafficked primarily to the South Asian countries such as such as Cambodia, Myanmar, Laos, and Thailand, and they are forced to commit cyber crimes. The targeted victims are coerced to commit target based cyber crimes such as digital arrest scams, investment scams, ponzi scams and romance frauds targeting people globally, including Indian citizens. They are kept in confinement, and physically abused if they did not meet the target crimes terming the whole process as cyber slaves.

Traditionally the human trafficking networks were dependent on physical exploitation techniques. Traffickers are now utilizing information and communication technologies (ICTs) to conduct transnational exploitation on a large scale, due to the advancement of global platform economies and cyber-physical systems.

The Case: Since last two years many cases have surfaced in the media about cyber slavery rackets and involvement of human transnational trafficking networks. The traffickers of the day have sharpened their operations by digital tradecrafts into private digital spaces and connections with networks across the globe to maximize profile.

Recently in November 2025, the Cyber Centre of Excellence (CCoE) of CID Crime, Gujarat Police arrested the kingpin of international cyber slavery racket who was supplying Indian skilled manpower by luring with big packages to Chinese cyber mafia at Myanmar's KK Park and Cambodia, mostly hubs located in South Asian countries. The youth victims were held hostage and then made to work as cyber slaves.

After technical investigation by the Gujarat Police, he was found to be connected to many sub agents in India. According to the Government statement; "He was managing more than 126 sub-agents. The accused was in touch with more than 30 Pakistani agents and had direct connections with the HR network of more than 100 Chinese and foreign companies, which were supplying people to the cyber-fraud scam camps." He had many deals with international networks to supply more youths as per demand. As a main player he was "managing and controlling the recruitment, trafficking routes, financial arrangements and cross-border connections for this entire international network".

In another major update the Delhi Police's Intelligence Fusion and Strategic Operations (IFSO) unit also arrested two suspects for recruiting and transporting youths to Myanmar. The Ministry of External Affairs in coordination with the Indian Airforce and in collaboration with Foreign Ministries of the host countries have carried out multiple rescue operations on number of occasions. According to the Rajya Sabha unstarred question no-1346 answered on 11/12/2025 Indian national rescued as per **(Table. 1)**

Sr. No.	**Country**	**No of Indian Nationals Rescued**
1	Cambodia	2,265
2	Lao PDR	2,290
3	Myanmar	2,165

Table 1: No of Indian nationals rescued

Evolving Modus Operandi: The youths were lured through various popular social media platforms as Telegram, Instagram, and Facebook, with the fake advertisement of high paying jobs. Once the fishing and recruitment was done the victims passport were seized, they were transferred to Chinese hubs like KK Park at the Myawaddy Township in Myanmar and forced to commit cybercrimes like phishing, crypto scams, Ponzi schemes and dating app fraud. Those who did not cooperate were allegedly subjected to physical and mental harassment.

III. Transnational and National Drugs Trafficking Rackets:

According to the UNODC drug trafficking is a global illicit trade involving the cultivation, manufacture, distribution, and sale of substances which are subject to drug prohibition laws.

Drug traffickers operating supply cross border and smugglers, mules operating within India in different states are adopting to digitally assisted modus operandi for execution, coordination, and supply of the contrabands. The criminal networks are using drones and encrypted communication platforms, technology, and dead drops methods alike to evade the law enforcement agencies.

The Case: The Narcotics Control Bureau (NCB) Chennai Zone has exposed a new modus operandi called 'dead drops' followed by a local

criminal gangs involved in supply of drug in the southern states. A dead drop is method in which the mule responsible for delivery of contraband leaves the illicit packet at an unsuspected place in a safe manner and shares the GPS location with the receiver who then take it further to the customer. The transit process takes places through secret communication applications that are hard to trace, through these advanced apps networks involved share the links, receive orders, and coordinate delivery with each other.

Use of drones as carrier of drugs on India -Pakistan border is another challenge the forces and law enforcement agencies are facing these days, the annual report of Narcotics Control Bureau 2024 highlights there is sharp rise in drones' sightings and recovery that come into India from Pakistan along the International border. This evolving modus operandi has replaced traditional smuggling methods.

The Smuggling in India report 2024-25 published by the Directorate of Revenue Intelligence (DRI) highlights use of cryptocurrency for illicit payments and transfer of proceeds of crime particularly in drug and gold smuggling cases has doubled in recent years, with stablecoins like USDT increasingly replacing traditional hawala networks to turn to more conceal and hidden transactions. The cryptocurrencies due to its borderless nature enable organized criminal networks go anonymous and ensure hard-to-trace international transfers, bypassing formal financial systems.

3. Analysis: Connecting the Dots

All the three highlighted evolving case studies of TOC, arms smuggling, cyber slavery, and drugs trafficking rackets reveals an interconnected pattern of digital and physical transition for commission of organized crimes. Commonality in use of digital spaces in terms of use of drones, dead drops, private secret encrypted communication platforms, social media all to avoid detection and conceal the network identity from the law enforcement agencies.

Anonymity by Criminals: The Space Transition Theory of Cyber Crime by (K Jaishankar, 2008) explains cyber space crimes. From the above case studies the organized criminal's transit between physical and cyber spaces such as the drones execute physical drops (arms and drugs from Pakistan,

across international borders) the gang members coordinate with each other via private encrypted apps. Similarly in cyber slavery racket the recruitment of victims happens via Telegram, Instagram, Facebook leading to physical confinement in Myanmar/Cambodia. The change of GPS location for dead drops of drugs and change of patterns for drop of arms suggest sophisticated operational planning by organized criminals' groups to execute the crimes. Cyber space also promotes to unite strangers online (e.g., links of Indian cyber slavery kingpin with Pakistani agents with Indian handlers, Chinese mafia with local kingpins) for demand of talent to run the cyber hubs.

Use of encrypted communication platforms is one of the common links between various organized crime and terrorist groups for enabling their operations. Such highly conceal apps are used to share maps, locations, layouts, important documents, and instructions that is private and exclusive to the group members only. For instance, in the Delhi terror blast that took place in November 2025 near Red Fort, based on the investigation it was found the arrested terror group members were communicating with each other through encrypted communication platforms. The accused used a combination of Telegram, Signal, Threema, and Session apps to coordinate with handlers abroad. These apps provide strong encryption, privacy and anonymity features encouraging their use by organized criminals and terrorist.

Investigators face challenges to track the communications due to end-to-end encryption. Messages can be seen only by the sender & receiver, even the companies cannot access the message content.

4. Rethinking Counter Policing Strategies: Strengthening Police Response

As the organized criminals gone advanced shading conventional operational approach to more advanced digitally assisted and technology driven operations, policing the activities of international and national organized syndicates requires rethinking investigative counter strategies to fight the organized crime. The existential policing crime prevention methods, such as neighbourhood watch programs, random stop-and-search

initiatives, and foot patrols, community policing schemes alongside technological approaches, such as surveillance systems, crime mapping, and geographical profiling are noteworthy in arresting low operative criminals and lead to paucity of operations for a brief period of time but not busting the entire organized network and their activities due to its sophistication, anonymity, and evolving modus operandi. Based on the cases discussed above the policing initiatives can be considered as given below:

4.1 Use of Artificial Intelligence (AI):

Artificial Intelligence (AI) has changed many industries and sectors, including criminal justice, security forces and crime and criminality. AI is used by criminal organizations, syndicates in the same ways that it is used by legitimate agencies and companies for supply chain management, risk assessment and mitigation, personnel selection, social media data mining, and various types of analysis and problem solving. Some crime syndicates have operations on all six civilized continents, and now AI is helping them to run those operations more efficiently than ever. AI has the potential to revolutionise crime prevention and detection through its subfields, such as machine learning and computer vision. Machine learning algorithms can process large amounts of data to forecast potential criminal activity, thus transforming law enforcement operations. Computer vision models can utilise visual data from surveillance cameras and other sources to analyse, identify, and respond to crimes.

- **Link Analysis Chart:** One of the most useful applications of AI in countering organized crime is with link analysis chart, providing visual representations of organizational hierarchies and activities to clarify the nature of criminal networks. AI enables investigators and analysts to process massive amounts of data in seconds, revealing patterns, trends and connections that even a skilled human eye can miss to identify criminals purchase patterns, money trail patterns, track consignments, and contrabands.
- **The South American Drug Cartel Disruption using AI:** A federal South American police force used AI-powered investigative solutions to disrupt international drug cartel operations. They used AI to follow

financial trails and seize assets owned by the kingpins. Using tools like Cellebrite Pathfinder and UFED Cloud (now Inseyets), investigators extracted and analysed data from digital devices, uncovering key connections between suspects, bank accounts and physical assets. The operation resulted in the arrests of 45 individuals, the seizure of $400 million worth of assets and disruption of a major drug-smuggling network.

- **MARVEL AI the Maharashtra Police Model:** Government has set up a Special Purpose Vehicle (SPV) named Maharashtra Advanced Research and Vigilance for Enhanced Law Enforcement (MARVEL) in 2024 an initiative to strengthen the modern day police intelligence, improve crime prediction and modernise investigation methods, making Maharashtra the first state in India to create an independent AI body for law enforcement. Mr. Harssh A Poddar, Superintendent of Police, Nagpur (Rural), the ex-officio Director and Chief Executive Officer say "Our mission is to augment — not replace — human policing." The AI tool is used to track the digital trace of criminals, detect patterns and focus on predictive policing. Besides the tool is also used to resolve human animal conflicts by minimising wildlife and human accidents and deaths. Lastest on December 12, 2025 the MARVEL launched MahaCrimeOS AI, a customised tool cocreated by Microsoft. It aids officers process complaints faster, analyse complex data, and follow investigative procedures more efficiently, capabilities that are essential in cybercrime cases. In complex cases such as narcotics and crime against women the AI copilot generates an investigation plan immediately, guiding officers on the next steps, which statements to record, which bank accounts to freeze and what social media profiles to examine.
- **The Uttar Pradesh Crime GPT Model:** The UP police are utilizing AI tools to catch criminals, the Crime GPT, created by Staqu Technologies. It aids the police department by using the digital database of criminals with features, such as recognising faces and voices and analysing criminal gangs.

4.2 Anti Drone Systems the Punjab Model: The Punjab Government launched Anti Drone Systems called 'Baaz Akh' (Hawk Eye) to counter the cross border smuggling of arms and drugs. The drones are deployed at specific border points where high drone activity has been observed. The system is equipped to accurately detect the upcoming enemy drone's position and its ground control stations.

It has an automated alert technology, which immediately notifies authorities upon detecting drone movement, thus eliminating the need for manual monitoring. This is considered the second line of defence alongside the Border Security Force on the Indo-Pak border.

4.3 Behavioural Analytics: Behavioural analytics is the proactive use of data to identify anomalies in human behaviour patterns to detect and prevent potential risks. The police specialized units should be trained in behavioural analytics to study and understand criminal syndicate behaviour on digital platforms to generate cues to profile criminals, their skills and motivation to track their online behaviour, data access, communication patterns, and "social signals" from digital traces to infer characteristics, networks, and intentions of actors and their future moves. The findings from multidisciplinary intelligence should be shared across agencies to take timely actions.

4.4 Strengthening Cyber Forensic Architecture: The end-to-end encrypted instant messaging services has provided criminals involved in international organized crime with high-tech tools to contact each other in a secure manner. The specialized cyber police units should be trained in advanced cyber forensic tools and techniques such as in-memory analysis and side-channel attacks to break the encrypted messages on devices. For cryptocurrency transactions cryptographic key recovery techniques for analysing the suspect's digital footprint and leveraging known vulnerabilities in cryptocurrency wallets to crack the cases.

5. Limitation of the Study:

The study relies on secondary media and public reports, which may not capture classified details or full investigative outcomes. Real-time primary

data access was unavailable, potentially limiting depth on operational intricacies or long-term syndicate disruptions.

6. Conclusion:

The Transnational Organized Crimes have taken a new shape in intersection of physical and digital spaces that adds new challenges to law enforcement agencies across the world. The evolving modus operandi demands a multifaceted approach. Technological advancements proactive, tech-integrated policing to dismantle networks exploiting anonymity in cyberspace and physical borders. Implementing AI for predictive analytics, anti-drone defences, and cyber forensics, alongside inter-agency intelligence sharing, can neutralize threats like those in the analysed arms, cyber slavery, and drug rackets. While these strategies show promise as evidenced by MARVEL AI's investigative acceleration and Punjab's anti drone interceptions, sustained capacity building training and ethical oversight are essential for efficacy thus ensuring security and peace in the region.

References:

1. *Awasthi, S. (2024, July 1). The dark web as enabler of terrorist activities. orfonline.org.https://www.orfonline.org/research/the-dark-web-as-enabler-of-terrorist-activities*
2. *Ayush.Sharma.Cs. (n.d.). History of cyber crime in India. Scribd. https://www.scribd.com/document/861933415/History-of-Cyber-Crime-in-India*
3. *Behavioral Analytics - NICE Actimize. (n.d.). https://www.niceactimize.com/glossary/behavioral-analytics#:~:text=What%20is%20Behavioral%20Analytics?,their%20security%20and%20operational%20efficiency.*
4. *Cyber Slavery Infrastructures: A Socio-Technical Study of Forced Criminality in Transnational Cybercrime. (n.d.). https://arxiv.org/html/2510.12814v1#:~:text=The%20rise%20of%20%E2%80%9Ccyber%20slavery,with%20Indian%20law%20enforcement%20agencies.*

5. *Deshkar, A. (2025, December 14). Satya Nadella launches AI-powered tool for Maharashtra police: How will it change crime investigation in state. The Indian Express. https://indianexpress.com/article/explained/mahacrimeos-ai-maharashtra-10418600/*
6. *Desk, T. T. (2024, September 24). How law agencies from 9 countries took down communications platform used for drug trafficking, money laundering. The Times of India. https://timesofindia.indiatimes.com/technology/tech-news/how-law-agencies-from-9-countries-took-down-communications-platform-used-for-drug-trafficking-money-laundering/articleshow/113467311.cms*
7. *Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. Trends in Organized Crime, 1–20. https://doi.org/10.1007/s12117-022-09457-y*
8. *Express News Service. (2025a, November 19). Mastermind' of 'cyber slavery' racket arrested: Gujarat Police. The Indian Express. https://indianexpress.com/article/cities/ahmedabad/mastermind-of-cyber-slavery-racket-arrested-police-10373294/*
9. *Express News Service. (2025b, November 23). Delhi Police bust Myanmar cyber-slavery racket, arrest two recruiters. The New Indian Express. https://www.newindianexpress.com/cities/delhi/2025/Nov/23/delhi-police-bust-myanmar-cyber-slavery-racket-arrest-two-recruiters*
10. *Gundy, M. (2025, July 29). Practical AI: Real-world applications and limitations in law enforcement. Police1. https://www.police1.com/police-products/investigation/investigative-software/practical-ai-real-world-applications-and-limitations-in-law-enforcement*
11. *Harpreet Bajwa. (2025, December 2). BSF rolls out advanced AI-based anti-tunnelling, anti-drone systems along Indo-Pak border. The New Indian Express. https://www.newindianexpress.com/nation/2025/Dec/02/bsf-rolls-out-advanced-ai-based-anti-tunnelling-anti-drone-systems-along-indo-pak-border*
12. *Jha, R. S. (2025, November 22). ISI-linked arms racket busted: 10 high-end foreign pistols, Turkiye-made PX-5.7 pistol, 92 live cartridges seized; smuggled from Pakistan via drones. The Times of India. https://timesofindia.indiatimes.com/city/delhi/isi-linked-arms-racket-*

busted-10-high-end-foreign-pistols-92-live-cartridges-seized-smuggled-from-pakistan-via-drones/articleshow/125499345.cms

13. *Lampe, K. V. (2016). Organized Crime Analyzing illegal activities, criminal structures and extra legal governance. SAGE.*
14. *Marvel | Home Department | India. (n.d.). https://home.maharashtra.gov.in/en/marvel/*
15. *Meet Crime GPT, the UP Police Department's AI tool for fighting crime. (n.d.). IndiaAI. https://indiaai.gov.in/article/meet-crime-gpt-the-up-police-department-s-ai-tool-for-fighting-crime*
16. *Pti. (2025a, August 9). Punjab launches anti-drone systems to tackle cross-border smuggling. The Times of India. https://timesofindia.indiatimes.com/india/punjab-launches-anti-drone-systems-to-tackle-cross-border-smuggling/articleshow/123207440.cms*
17. *Pti. (2025b, September 16). Drug-laden Pak drones significant threat to Indias internal security: NCB report - The Tribune. The Tribune. https://www.tribuneindia.com/news/punjab/drug-laden-pak-drones-significant-threat-to-indias-internal-security-ncb-report/#:~:text=%22The%20use%20of%20drones%20for,methaqualone%20abused%20mainly%20by%20youngsters.*
18. *Pti, Pti, & Chronicle, D. (2025a, December 4). Deccan Chronicle. Deccan Chronicle. https://www.deccanchronicle.com/news/crypto-stablecoins-being-used-to-fund-drug-gold-smuggling-racket-dri-report-1921618*
19. *QUESTION NO-1346 REPATRIATION OF CITIZENS FALLEN VICTIM TO CYBER SLAVERY. (n.d.). Ministry of External Affairs, Government of India. https://www.mea.gov.in/rajya-sabha.htm?dtl/40442/QUESTION+NO1346+REPATRIATION+OF+CITIZENS+FALLEN+VICTIM+TO+CYBER+SLAVERY*
20. *S, V. (2025, July 11). Traffickers resort to 'dead drop' method to transit drugs. The Times of India. https://timesofindia.indiatimes.com/city/chennai/traffickers-resort-to-dead-drop-method-to-transit-drugs/articleshow/122393154.cms*
21. *Siddiqui, S. (2025, November 18). Delhi blast terror suspects used encrypted apps for secret communication: How terrorists use private apps l. Bhaskar English. https://www.bhaskarenglish.in/tech-science/news/delhi-car-blast-suspects-used-encrypted-apps-to-share-plans-136442786.html#:~:text=The%20car%20blast%20near%20Delhi%27s,doing%20to%20counter%20such%20misuse.*

22. *Tamboli, V. (2024). Forensic encryption: Discovering hidden digital secrets. Stechnolock Journal of Cryptology, 2(1), 1–7. https://www.stechnolock.com/article/Forensic-Encryption-Discovering.pdf*
23. *Team, T. (2025, October 30). Maharashtra uses AI to ensure safety and security without replacing humans. The Better India. https://thebetterindia.com/innovation/maharashtra-ai-marvel-smart-policing-malnutrition-wildlife-conflicts-traffic-management-10607541*
24. *Desk, T. T. (2024, September 24). How law agencies from 9 countries took down communications platform used for drug trafficking, money laundering. The Times of India. https://timesofindia.indiatimes.com/technology/tech-news/how-law-agencies-from-9-countries-took-down-communications-platform-used-for-drug-trafficking-money-laundering/articleshow/113467311.cms*
25. *Jha, R. S. (2025, November 22). ISI-linked arms racket busted: 10 high-end foreign pistols, Turkiye-made PX-5.7 pistol, 92 live cartridges seized; smuggled from Pakistan via drones. The Times of India. https://timesofindia.indiatimes.com/city/delhi/isi-linked-arms-racket-busted-10-high-end-foreign-pistols-92-live-cartridges-seized-smuggled-from-pakistan-via-drones/articleshow/125499345.cms*
26. *Pti. (2025, September 16). Drug-laden Pak drones significant threat to Indias internal security: NCB report - The Tribune. The Tribune. https://www.tribuneindia.com/news/punjab/drug-laden-pak-drones-significant-threat-to-indias-internal-security-ncb-report/#:~:text=%22The%20use%20of%20drones%20for,methaqualone%20abused%20mainly%20by%20youngsters.*
27. *Pti, Pti, & Chronicle, D. (2025, December 4). Deccan Chronicle. Deccan Chronicle. https://www.deccanchronicle.com/news/crypto-stablecoins-being-used-to-fund-drug-gold-smuggling-racket-dri-report-1921618*
28. *Siddiqui, S. (2025, November 18). Delhi blast terror suspects used encrypted apps for secret communication: How terrorists use private apps l.Bhaskar English. https://www.bhaskarenglish.in/tech-science/news/delhi-car-blast-suspects-used-encrypted-apps-to-share-plans-136442786.html#:~:text=The%20car%20blast%20near%20Delhi%27s,doing%20to%20counter%20such%20misuse.*

Author's Profile

Mr. Parvesh is working as Deputy Assistant Director (Lecturer Social Sciences) at the North Eastern Police Academy, Ministry of Home Affairs, Government of India. Previously, he had worked as Assistant Professor of Criminology and Security Studies at the Rashtriya Raksha University, INI, Ministry of Home Affairs, Government of India, Gandhinagar, Gujarat and as Forensic Professional (Forensic Psychology Division) at Central Forensic Science Laboratory, Pune, Ministry of Home Affairs, Govt of India, and he has also worked as an Analyst, with a Not-for-Profit Trust on a special project on Crime Against Women and Children.

He holds a Master's degree in Criminology and Master's degree in Psychology and a Bachelor of Science degree in Forensic Science.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.2, (P. 144-157)

Leveraging Machine Learning for Enhanced Fake Profile Detection on Facebook

Dr Priya P Sajan*

Abstract:

The increasing prominence of social media has significantly transformed social interactions in recent years, encouraging individuals to participate across multiple platforms. Globally, people are highly active on social media, yet this landscape is also plagued by the presence of fake profiles. This research project leverages various machine learning techniques to differentiate between fake and genuine Facebook profiles. The analysis is based on features such as the number of posts, unaccepted friend requests, likes on unknown accounts, daily comments, and additional relevant attributes. To tackle the issue of fake accounts on social media, we implement several machine learning algorithms and subsequently assess the effectiveness of Random Forest, K-Nearest Neighbors (KNN), and Support Vector Machines (SVM) in accurately identifying these fraudulent profiles.

Keywords: *Fake Profile, Social Network Analysis, Machine Learning Algorithms, Fraud Detection, Facebook Security*

I. Introduction:

Social media profile is a personal page on a social media platform that allows users to connect, share content, and interact with others. It usually features details like the user's name, photo, bio, and interests, acting as a

* *Senior Project Engineer C-DAC*

digital representation of the person. These profiles enable both individuals and businesses to establish their presence online, engage with their audience, and promote their personal or professional brands. Furthermore, social media profiles play a crucial role in data analytics, targeted advertising, and understanding user behavior, making them essential components of the digital landscape.

Fake profiles are created with false information, designed to deceive others by using fabricated names, photos, and personal details. These profiles often serve malicious purposes, such as spreading misinformation, scamming people, or engaging in fraudulent activities. The presence of fake profiles can lead to several disadvantages, including the dissemination of false information and fake news, which misleads users and fosters confusion. They can also facilitate scams, tricking individuals into divulging personal information or money. Users become less confident in social media platforms as a result of the prevalence of false profiles, which also cause users to doubt the veracity of other accounts. Additionally, fake profiles can be used for cyberbullying and harassment, causing emotional harm, and they pose a threat to data privacy by collecting personal information under false pretenses.

Fake profiles have the potential to significantly affect society by affecting many facets of trust and social interaction. In 2023, the Federal Trade Commission (FTC) reported that scams originating from social media platforms resulted in $2.7 billion in losses. Scammers utilise these sites to market phoney investment opportunities, unfilled orders, and romance scams by creating fake profiles or hacking into accounts. These scams are particularly effective at attracting younger audiences because a significant percentage of their victims are in the 18 to 29 age range. Fraudulent schemes frequently involve misleading ads for products and deceptive investment, particularly those related to crypto currency. Tackling the effects of fake profiles demands coordinated efforts from social media platforms, policymakers, and users to uphold online integrity and foster a safer digital space. As social media platforms become more popular, they provide users with extensive data, which also attracts malicious actors.

The large amounts of data available make these platforms attractive targets for fake accounts. Recent incidents of fraudulent profiles highlight the ongoing difficulties in verifying online identities and building trust. These problems include the misuse of fake social media personas for political manipulation and influencing public opinion. Additionally, scams that leverage fake profiles can endanger consumers' personal and financial security. To combat these issues, social media platforms employ user reporting systems and AI-based detection tools to identify and remove fake accounts. Nonetheless, the continued existence of these profiles raises broader concerns about cyber-security, privacy, and trust in the digital realm. Addressing these issues requires a collaborative effort among tech companies, legislators, and users to strengthen online safety measures while maintaining the transparency and connectivity of social media.

In 2023, approximately 4.9 billion people globally are active on social media. Facebook remains the leading platform worldwide, boasting 2.9 billion monthly active users. Among the countries, India has the highest number of Facebook users, with an impressive 448.1 million individuals. Current statistics indicate that India has 260 million registered Facebook users, the largest figure globally, while the United States follows with 180 million registered users. Figure 1 illustrates the global user statistics for major social networking sites, including Twitter,

Facebook, YouTube, and WhatsApp.

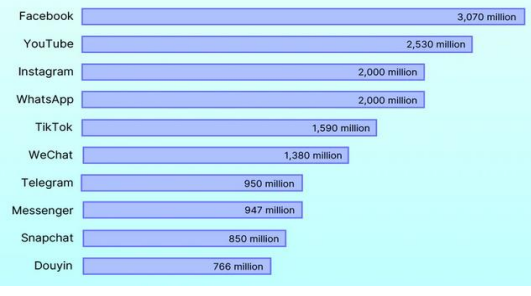


Fig.1 Global usage statistics of major social media platforms (in millions of active users) in 2025

The fake profile issue is present on all popular Open Storage Network websites such as FB having 1.3 billion fake profiles. Many pieces of research have focused on detecting spam messages. However, identifying fake profiles on social networking websites remains a significant

challenge. These fake profiles are often created by stealing data from existing profiles on the network, such as profile names, photos, age, sex, and other information that is easily accessible. This situation can result in huge damage in the real world, including citizens, business entities, and others.

II. Proposed System:

This research aims to present up-to-date research work on fake account detection. By using machine learning algorithms to identify and mitigate the effects of an attack on a platform like Facebook. The proposed system leverages machine learning algorithms, specifically focusing on ensemble methods like Random Forest and KNN and SVM, to enhance the accuracy and efficiency of fake profile detection on social media platforms.

A. Data Collection:

The dataset used in this study consists of 1,000 Facebook user profiles, comprising both genuine and fake accounts. Since direct access to the Facebook Graph API is restricted due to privacy policies, the dataset was constructed using publicly available profile information, manually verified accounts, and synthetically generated data based on typical Facebook behavior patterns reported in prior literature. The dataset includes numerical and categorical features such as number of posts, follower count, unaccepted friend requests, and daily comments. All data was anonymized to ensure privacy. The dataset was then labeled into ‘fake’ and ‘genuine’ categories based on predefined behavioral criteria validated by domain experts.

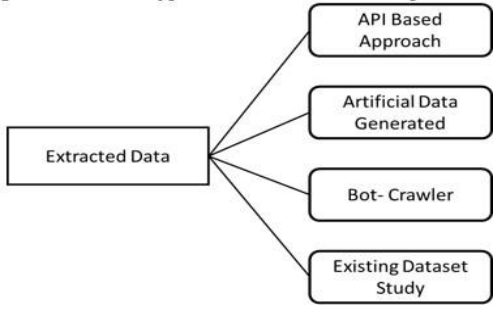


Fig.2: Data collection

B. Feature Description:

To detect the fake profiles on Facebook, there was various features related to the user's account and their posts are used (Table I). The features are defined as follows:

TABLE I
FREQUENTLY USED FEATURES

Categorical	full name gender
	email
	location
	relationship status education level profile picture
Numerical	No Of Post
	No Of Rejected Friend Requests
	No Of Friend Requests That Are Not Accepted
	No Of Friends
	No Of Followers
	No Of Likes To Unknown Account
	No Of Comments Per Day

1. Username: The username serves as the unique identifier for a user's account. Consequently, each user on the social networking site has a distinct name.
2. Profile_picture: A critical component of every social networking website is the profile photo associated with users' accounts. Profile visitors often identify individuals by viewing their photos, which can sometimes lead to mistakenly believing the photos are authentic, potentially resulting in deception.
3. Number of posts: This feature can help identify fake profiles, as an unusually high or low number of posts may indicate atypical user behavior. For instance, a genuine user is likely to have a consistent

posting history, while a fake profile might exhibit an irregular or artificially inflated posting frequency.

4. Number of friend requests that are not accepted: This indicator can assist in identifying fraudulent accounts, as an unusually high rate of rejected friend requests might suggest suspicious or inauthentic behavior, potentially indicating the presence of a fake or bot account.
5. Number of followers : It is defined as the number of existing profiles that are following the user's profile. In terms of Facebook, this corresponds to the number of friends or followers a user has, which can be used as a factor in identifying whether a profile is genuine or fake.
6. Number of likes to unknown accounts : Measures the frequency with which a user interacts with profiles that are not known to them. This metric can be used to help identify whether a profile is genuine or fake, as an unusually high number of likes to unknown accounts may indicate suspicious behavior typical of fake or automated accounts.
7. Number of rejected friend requests : feature tracks how many friend requests a user has rejected. This metric can be used to assess profile authenticity, as an unusually high number of rejected friend requests might suggest non-genuine behavior, potentially indicating a fake or suspicious account.
8. Number of comments per day : feature tracks the average number of comments a user posts daily. This metric can be useful for identifying fake profiles, as an unusually high or low volume of comments compared to typical user behavior may suggest automated or suspicious activity, which is characteristic of fake or bot accounts.

C. System architecture:

The proposed system analyzes user profile features to assess reliability on social networks. It integrates three distinct machine learning models—K-Nearest Neighbors (KNN), Random Forest, and Support Vector Machines (SVM)—into its architecture to manage data processing and classification tasks efficiently. The dataset undergoes preprocessing with various Python

libraries, and a comparison of models is conducted to identify the most effective algorithm for the dataset. The system aims to detect fake accounts on social media platforms using various machine learning techniques.

The model can easily read the extracted characteristics that were saved in a CSV file. Finally, whether a profile is genuine or not is finally determined by the training, testing, and analysis of the model. Before the dataset is delivered to a model, it is preprocessed. This approach seeks to determine whether a profile is genuine or fraudulent based on its look. All the specific details are now established. The categorical aspects have been eliminated, leaving only the numerical data. In this paper the features such as Number Of Posts, Number Of Rejected Friend Requests, Number Of Friend Requests That Are Not Accepted, Number Of Friends, Number Of Followers, Number Of Likes To Unknown Account, Number Of Comments Per Day, are used to train the model for predicting if it's fake or not. Dataset includes features such as 'No Of Post', 'No Of Rejected Friend Requests', 'No Of Likes To Unknown Account' etc.

In preprocessing step includes encoding categorical variables, scaling numerical features, and splitting the data into training and testing sets. The training dataset is used to train the machine learning model. The model learns patterns, relationships, and structures within this data. In this research paper the training is split into 70-80%. During training, the algorithm adjusts its internal parameters based on the input features and corresponding labels to minimize the error in its predictions. After training, the model makes predictions on the testing data, and these predictions are compared against the actual labels to compute performance metrics like accuracy, precision, recall, F1 score, and ROC-AUC.

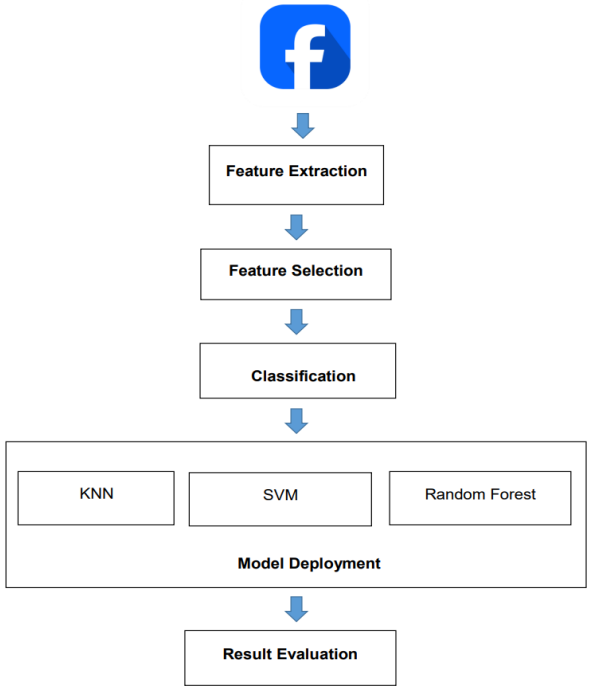


Fig. 3. System architecture

Random Forest (sometimes called random-decision forest) is an ensemble learning strategy that exemplifies this kind of technology. Similar to Figure 4, the Random Forest Forecasts the outcome based on the votes of the majority of predictions, using predictions from each decision tree instead of relying just on one. Random Forest, however, creates many more decision trees than the decision tree method does, and the final result seems to be the sum of nearly all of decision trees that have been created. For profile detection, the author employed the Random Forest method.

The Random Forest classifier is trained using the provided training data, where it identifies patterns and correlations between various features (such as the number of posts, number of friends, etc.) and the target variable (Fake or Not). Once trained, the model is applied to new, preprocessed data. It uses the previously learned patterns and relationships to predict whether each profile is genuine or fake. The effectiveness of the model is assessed using performance metrics like accuracy, precision, recall, and F1 score.

III. Experimental Results and Discussion:

The outcomes of each model's training and testing are as follows. The proposed model utilizes an artificially created dataset and analyzes a range of features to detect fake profiles on Facebook. The model examines various aspects of user activity, including the number of posts, number of rejected friend request, number of friends, number of followers, likes to unknown accounts, and the number of comments per day. By leveraging these features, the model aims to identify patterns indicative of fake profiles.

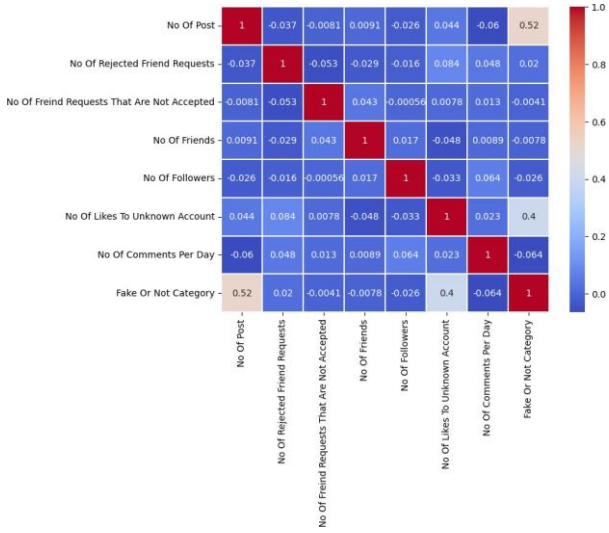


Fig. 4. Correlation matrix

Fig.4 shows a heatmap of a correlation matrix that shows the relationships between several variables. The correlation coefficient between two variables is displayed in each heatmap cell and can vary from -1 to 1. The intensity and direction of the correlations are shown by the colour scale on the right, where red denotes a strong positive connection, blue denotes a strong negative correlation, and white denotes no correlation. For example the feature No Of Post, positively correlated with" Fake Or Not Category" (0.52), indicating that as the number of posts increases, there is a tendency for the account to be categorized as fake. Weak or negligible correlations

with other variables, ranging from -0.06 to 0.044. And the feature, No Of Rejected Friend Requests is very weak correlations with other variables, the highest being with ”No Of Likes To Unknown Account” (0.084) and ”Fake Or Not Category” (0.02). This correlation helps to identifying which variables have stronger relationships with each other, which is particularly useful for feature selection and understanding underlying patterns in the data.

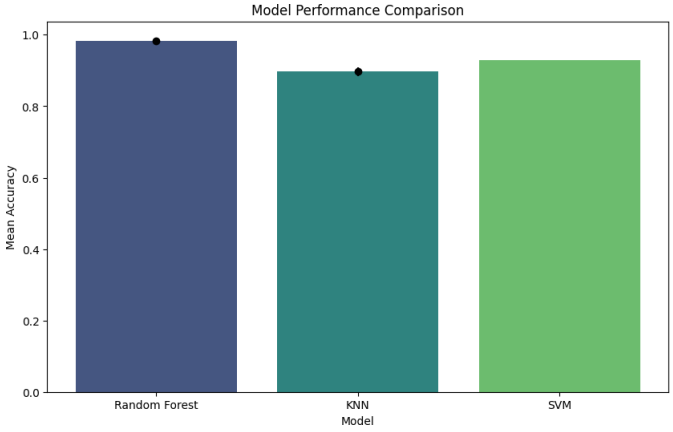


Fig. 5. Performance analysis

Fig.5 indicates performance of different models. Three machine learning models are compared in terms of mean accuracy: Random Forest, K-Nearest Neighbours (KNN), and Support Vector Machine (SVM). Random Forest model shows the highest mean accuracy, close to 9.8, indicating it is the most accurate model among the three for detecting fake images on Facebook. Each bar has a black dot near its top, likely representing the mean accuracy value or a specific statistical measure such as a confidence interval or standard deviation. KNN (90%) and SVM (93%) also perform well, but their mean accuracies are slightly lower than that of Random Forest.

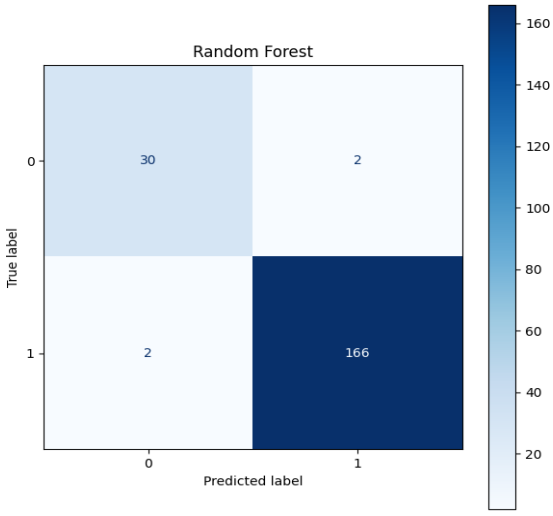


Fig. 6. Confusion matrics of random forest

This research paper focuses exclusively on the Random Forest classifier. Figure 6 presents the confusion matrix for this model. The Random Forest model accurately detected 166 fake identities, demonstrating a true positive rate of 166. Additionally, the model correctly identified 30 genuine profiles, representing the true negative rate. However, it incorrectly classified 2 genuine profiles as fake, resulting in a false positive rate of 2, also known as a Type I error. Conversely, when the model misclassified 2 fake profiles as real, it resulted in a false negative rate of 2, or a Type II error.

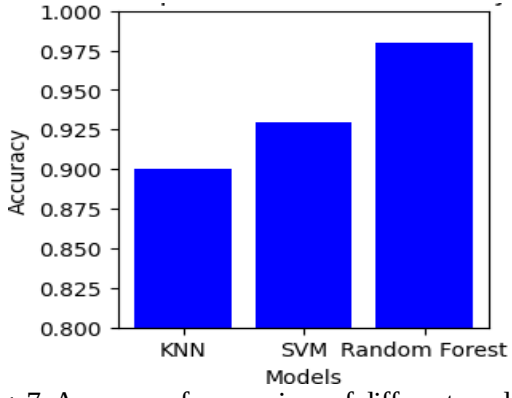


Fig. 7. Accuracy of comparison of different models

For the Random Forest model, both precision and recall are approximately 0.988, resulting in an F1 Score of 0.988 (or 98.8%). This high F1 Score indicates that the model is highly effective in correctly identifying fake identities with minimal errors. Specifically, the recall value of 0. 98.8 means that out of all the actual fake accounts, 98.8% were correctly identified by the model, demonstrating its robustness in capturing the majority of fake identities and ensuring that only a small percentage are missed. When comparing Facebook with the Random Forest classifier to other classifiers, there was a small predominance in the overall average accuracy of 0.98 obtained in the analysis, as shown in Fig. 7. Additionally, SVM have an accuracy of about 0.93 and the KNN have an accuracy of about 0.90. Various algorithms for machine learning are compared in this study to show which ones produce the best results (Random Forest 98%), even though those results are higher (98%) than those of the previous spam word list-based method (91.1%).

IV. Conclusion:

Fake accounts have continuously changed over time to evade detection. Therefore, developing techniques to identify bogus accounts is crucial. The objective of the research work is to find the fake profiles/identites on facebook. Due to the significant difficulty in gathering data due to Facebook's fine-grained privacy restrictions, the study used artificially generated datasets for Facebook features.

The proposed model utilizes a dataset derived from Facebook, incorporating features such as posts, comments, like patterns, unaccepted friend requests, and follower counts. The project employs widely used machine learning classification techniques to identify the most effective classifiers. This research focuses on three distinct machine learning models: K-Nearest Neighbors (KNN), Support Vector Machines (SVM), and Random Forest. Analysis revealed that the Random Forest model achieved the highest accuracy at 98%, outperforming the other models. The results indicate that the models are well-calibrated to handle the complexity of the dataset, validating the chosen features and preprocessing methods. The high accuracy rate supports the effectiveness of our

approach, highlighting its potential for practical applications in combating fraudulent activities and enhancing online security.

V. Future Research Directions:

In the future, integrating Q-Learning, Autoencoders (AEs), and Generative Adversarial Networks (GANs) could enhance performance. This will help to continuously increase accuracy in a variety of social media contexts. One significant area of focus is the detection of cloned profiles. Cloned profiles, which involve the duplication of genuine profiles with minor alterations, present a unique challenge. Addressing this issue would require advanced techniques for distinguishing between closely related profiles and identifying subtle discrepancies.

References:

1. *Roy, Pradeep Kumar, and Shivam Chahar. "Fake profile detection on social networking websites: a comprehensive review." IEEE Transactions on Artificial Intelligence 1.3 (2020): 271-285.*
2. *Sansonetti, Giuseppe, et al. "Unreliable users detection in social media: Deep learning techniques for automatic detection." IEEE Access 8 (2020): 213154-213167.*
3. *Van Der Walt, Este´e, and Jan Eloff. "Using machine learning to detect fake identities: bots vs humans." IEEE access 6 (2018): 6540-6549.*
4. *Aditya, Bhrugumalla LVS, and Sachi Nandan Mohanty. "Heterogenous Social Media Analysis For Efficient Deep Learning Fake-Profile Identification." IEEE Access (2023).*
5. *K. L. Arega and E. Shewa, "Social media fake account detection for Amharic language by using machine learning," Global Sci. J., vol. 8, no. 6, pp. 1–11, 2020*
6. *Balogun, A. B. J. Omar, M. Jabar, and M. M. Abdulmajid, "Spam detection issues and spam identification of fake profiles on social networks," J.Theor. Appl. Inf. Technol., vol. 95, pp. 5881–5895, Mar. 2017.*
7. *Roy, Pradeep Kumar, and Shivam Chahar. "Fake profile detection on social networking websites: a comprehensive review." IEEE Transactions on Artificial Intelligence 1.3 (2020): 271-285.*
8. *M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Towards detecting compromised accounts on social networks," IEEE Trans. Dependable*

Secure Comput., vol. 14, no. 4, pp. 447–460, Jul./Aug. 2017.

9. *Harris, Preethi, et al. "Fake instagram profile identification and classification using machine learning." 2021 2nd Global Conference for Advancement in Technology (GCAT). IEEE, 2021.*
10. *D. Yuan et al., "Detecting fake accounts in online social networks at the time of registrations," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2019, pp. 1423–1438.*

Author Profile's

Dr. Priya P. Sajan is a Senior Project Engineer at the Centre for Development of Advanced Computing (C-DAC), with experience in Cyber Forensics and Cyber Security. Her expertise spans cyber forensic investigation, incident response, digital evidence handling, and cyber threat management. She has contributed to several national-level projects. Her research interests include Drone Forensics, Ethical Hacking, Malware Analysis, Artificial Intelligence, Machine Learning, IoT Security, and Cyber Threat Handling & Incident response.

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