Sardar Vallabhbhai Patel National Police Academy

Hyderabad

Technology Special Newsletter

Sardar Vallabhbhai Patel National Police Academy

Hyderabad

Technology Special Newsletter

Published by

Director
SVP National Police Academy
Shivramapalli, Hyderabad -500 052

Ph: (040) 24015151-58, Fax (040) 24015179

Website: www.svpnpa.gov.in,

Email: publication sec@svpnpa.gov.in,

Director's message

Shri Amit Garg
Director, NPA

It gives me immense pleasure that the Sardar Vallabhbhai Patel National Police Academy is bringing out this Newsletter documenting the key deliberations of the Workshop on "Use of Technologies in Policing – Learning from Each Other" conducted from 16th to 18th March 2026.

The workshop provided a valuable platform for officers, experts and practitioners to exchange ideas and best practices relating to technology-enabled policing. Important themes such as Artificial Intelligence in investigation, cybercrime investigation, drone technology, communication systems, CCTNS & ICJS integration and aviation security were deliberated upon during the programme.

This Newsletter captures the important presentations, discussions and operational experiences shared during the workshop. I am confident that this publication will serve as a useful reference for police officers and practitioners working in the field of technology-driven policing.

I appreciate the efforts of the Course Director, faculty members, contributors and participating officers for making both the workshop and this publication meaningful and successful.

The ready reckoner compilation of significant technological initiatives and best practices presented by participating organisations included in this publication will further facilitate knowledge sharing and professional learning among police organisations.

I hope this publication will further promote innovation, collaboration and effective use of technology in policing.

Course Director's message

Shri Ilango R, IPS
Assistant Director, NPA

It gives me immense pleasure to place on record the successful conduct of the workshop on "Use of Technologies in Policing – Learning from Each Other" at the Sardar Vallabhbhai Patel National Police Academy. The workshop brought together officers from various States, UTs, CPOs and CAPFs, creating a meaningful platform for exchange of practical knowledge, field experiences and technology-driven innovations in policing.

The central idea of the programme was not merely to discuss technology in theory, but to understand how it is being applied in real policing situations. The sessions on Artificial Intelligence, drone technology, cybercrime investigation, communication systems, data integration, digital forensics, citizen services, traffic management and operational tools reflected the growing importance of technology as a force multiplier in modern policing. The panel discussions, technical sessions, tech exhibition and experience-sharing exercises helped participants appreciate both the opportunities and the challenges involved in adopting new technologies.

This newsletter is a logical conclusion of the workshop. It has been prepared with the intention of collating, curating and presenting the key learnings, best practices, field-tested tools, expert insights and practical outcomes generated during the programme. By bringing these inputs together in a structured form, the newsletter seeks to disseminate the knowledge gained during the workshop to a wider audience within the policing and security community.

A particularly valuable aspect of this workshop was the spirit of peer learning. Officers shared tools, applications and best practices from their respective organisations, enabling others to identify tested solutions, avoid duplication of effort and adapt relevant technologies to local requirements. The participation of experts, practitioners, technology partners and IPS probationers further enriched the learning environment.

I sincerely appreciate the enthusiasm, discipline and active participation of all officers who contributed to the success of this programme. I also acknowledge the efforts of all speakers, moderators, exhibitors and supporting teams who made this workshop productive and outcome-oriented. I am confident that the knowledge and ideas captured in this newsletter will help police organisations move towards more efficient, citizen-centric, secure and technology-enabled policing.

Best wishes.

Contents

Section	Title	Page No.
	Executive Summary	**vii**
PART - I	**Key Outcomes of the Workshop**	**1**
1.1	Field-Tested Policing Technologies — A Compendium of Solutions Adopted by States, CPOs and CAPFs	2
1.2.1	Artificial Intelligence in Investigation – Field-Level Applications	12
1.2.2	Drone Technology and Counter-Drone Preparedness	13
PART - II	**Brief Summary of Sessions**	**15**
2.1	Technology in Policing – Opportunities, Challenges and Limitations	17
2. 2	DRDO's Association with CAPFs, Police & BPR&D and Technologies for Internal Security	19
2. 4	Artificial Intelligence in Investigation – Field-Level Applications	23
2. 4. 1	From Reactive to Proactive Policing	24
2. 4. 2	AI as an "Ironman Suit" for Police	25
2. 4. 3	AI Ecosystem in Telangana Police	26
2. 4. 4	Best Practices & Experience Sharing in Maharashtra Police	28
2. 5	Drone Technology and Counter-Drone Preparedness	30
2. 5. 1	Basics of Drone Flight	30
2. 5. 2	Choosing the Right Techniques for Anti-Drones	34
2. 5. 3	Experience in Local Law Enforcement	35
2. 5. 4	Tech Initiatives in Kerala (Online)	38
2. 6	Mule Accounts Identification & Cybercrime Investigation	41
2. 7	POLNET & Public Protection Communication Systems	43
2. 8	Aviation Security and Emerging Threats	45
2. 9	IT Initiatives by SVPNPA/ Cyber X	47
2. 10	Problem-Driven Innovation in Policing: Goa Model	51
2. 11	Challenges in Technology Implementation in Policing & Its Experiences	54
2. 12	Cyber Auditor	57
2. 13	Presentation on CCTNS & ICJS	60
PART - III	**Tech Exhibition**	**63**
3. 1	Overview of Tech Exhibition	65
3. 2	Details of Tech Exhibition Products, Apps and Tools	67
3. 3	DRDO Developed Products	67

Sitting Left to Right S/Shri : Dr. Divya V. Gopinath, Manjunath. H, Kranthi Kumar Gadidesi, Dr M. Tamilvanan, DD (Works), Dr Rohini Katoch Sepat, DD (BC-I), Ilango R, AD (SC) & Workshop Director, Amit Garg, Director, SVP NPA, Vinit Dev Wankhede, M. Sree Abhinav, AD (OD), E Sai Charan Tejaswi, AD (IS-I), Ashim Sen, Rajesh Kumar Singh, Musadiq Majid Basu.

Standing Left to Right (1st Row) : Sanjeev Kumar Singh, Koli Sagar Dilip, Harsh Indora, Arshi Aadil, Dr. Priyanka Narnaware, Sulesh Choudhary, Dr. Vaishali Kadukar, G. L. Gouthami, Dara Kavitha, Mary G. T. Sangma, Vinay Barthwal, Akash Kumar Shukla, Avinash Mishra.

Standing Left to Right (2nd Row) : Abhishek Gupta, Sachin Sharma, P. S. Sreejith, R. Remliana, Kumar Chandra Bhanu Prakash, Romesh Yaikhom, Anil Chaudhary, V. Syam Babu, Sujeet Roy, Chennabasavanna. S. L, Joysar Hiteshkumar H, Manish Singh.

Glimpses from the Course

Panel Discussion on Drone Technology

Glimpses from the Course

Panel Discussion on AI in Investigation

Executive Summary

A 03-day Workshop on "Use of Technologies in Policing – Learning from Each Other" was conducted at the Sardar Vallabhbhai Patel National Police Academy from 16th to 18th March 2026, with participation from officers representing various States, UTs, CPOs and CAPFs. The workshop aimed to provide a common platform for sharing technological innovations, best practices and operational experiences in policing.

The primary objective of the programme was to highlight the role of technology as a force multiplier in policing and internal security. The workshop encouraged participating organisations to showcase applications and tools relating to cybercrime detection, station house management, citizen-centric services, intelligence and tactical operations, law and order management, crime detection, traffic management and immigration-related policing.

The inaugural sessions focused on the integration of technology in policing, including presentations on DRDO's association with police forces, opportunities and challenges in technology adoption for internal security, and the role of CCTNS and ICJS in modern policing. Senior officers from NCRB, DRDO and State Police organisations shared their perspectives on leveraging technology for efficient policing and inter-agency coordination.

Subsequent sessions covered a wide range of emerging technologies and operational practices. Key themes included the use of Artificial Intelligence in investigation, identification of mule accounts, PPDR and POLNET communication systems, aviation security, cybercrime investigation techniques, and technology initiatives undertaken by different States such as Goa and Kerala Police. Panel discussions enabled officers to exchange practical experiences and discuss challenges in implementation.

Special emphasis was laid on contemporary technological interventions such as drone technology, cyber auditing, and best practices in local law enforcement. Experts from police organisations, academia and the private sector delivered lectures and demonstrations on operational applications of technology in policing. The workshop also included a technology exhibition where participating agencies displayed innovative tools and applications for knowledge sharing and collaboration.

Overall, the workshop successfully provided a collaborative learning platform for police and security agencies to exchange ideas, showcase innovations and identify practical technological solutions for improving policing efficiency, investigation capabilities and service delivery.

Time Table of Use of Technologies in Policing – Learning from Each Other
(16th – 18th March, 2026)

<table>
<tr><td>Day/Date</td><td colspan="2">0930 - 1010 hrs</td><td colspan="2">1010 - 1110 hrs</td><td>1110 - 1130 hrs</td><td colspan="2">1130 - 1230 hrs</td><td>1230 - 1240 hrs</td><td colspan="2">1240 - 1330 hrs</td><td>1330 - 1500 hrs</td><td colspan="2">1500 - 1545 hrs</td><td>1545 - 1555 hrs</td><td>1555 - 1615 hrs</td><td>1615 - 1700 hrs</td><td>1700 hrs</td><td>1740 hrs</td></tr>
<tr><td>16.03.2026 (Monday)</td><td colspan="2">Joining Formalities</td><td colspan="2">Technology in Policing - opportunities, challenges and limitations

Shri Vinit Dev Wankade, IPS, DGP-CMD, Tamilnadu Police Housing corporation Ltd, Chennai</td><td>Group Photo & High Tea</td><td colspan="2">Technology in Policing - opportunities, challenges and limitations

Shri Vinit Dev Wankade, IPS, DGP-CMD, Tamilnadu Police Housing corporation Ltd, Chennai</td><td>bio break</td><td colspan="2">DRDO's Association with CAPFs, Police & BPR&D of MHA and Technologies for Internal Security

Shri A. Sangita Rao Achary, Director, DRDO-DLIC</td><td>LUNCH</td><td colspan="2">NATGRID Database for Policing: Data Sharing with LEAs

Shri B. Praveen, Joint Secretary, NATGRID</td><td>Tea Break</td><td>Experience Sharing by Participant

Shri Sujit Roy, Sr. Director, NTRO</td><td>Presentation on CCTNS & ICJS

(Online)

Shri Jayant Singh, IPS, AD, NCRB</td><td>Tech Exhibition</td><td>Round the Campus</td></tr>
<tr><td></td><td colspan="3">0930 - 1100 hrs</td><td>1100-1120 hrs</td><td colspan="2">1120 - 1155 hrs</td><td>1155 - 1200 hrs</td><td>1200 - 1245 hrs</td><td>1245-1250 hrs</td><td>1250 - 1330 hrs</td><td>1330 - 1500 hrs</td><td colspan="3">1500 - 1600 hrs</td><td>1600 - 1615 hrs</td><td colspan="4">1615 - 1715 hrs</td></tr>
<tr><td rowspan="2">17.03.2026 (Tuesday)</td><td colspan="4">Artificial Intelligence in Investigation:</td><td colspan="2" rowspan="2">Panel Discussion

Moderator: Shri Ajit Pratap Singh, IPS, DD (IT-2), SVP NPA

1. Ms. Mallika Garg, IPS, SP, AP
2. Shri K. Pratap SivaKishore, IPS, SP, AP
3. Shri Bhaskaran, IPS, DIG, TG</td><td rowspan="2">Bio Break</td><td rowspan="2">Panel Discussion</td><td rowspan="2">bio break</td><td rowspan="2">Mule Accounts Identification & Best Practices

Ms. Shahnaz Illyas, IPS, SP, Cyber Crime, TN</td><td rowspan="2">LUNCH</td><td colspan="3" rowspan="2">Presentations on POLNET & PPDR

Shri Ashim Sen, Joint Director, DCPW</td><td rowspan="2">Tea Break</td><td colspan="4" rowspan="2">Presentation on Aviation Security

Shri Senthil Avoodai Krishna Raj S, IPS, DIG, CISF</td></tr>
<tr><td colspan="3">Panel Discussion

Moderator: Shri Ajit Pratap Singh, IPS, DD (IT-2), SVP NPA

1. Ms. Mallika Garg, IPS, SP, AP
2. Shri K. Pratap SivaKishore, IPS, SP, AP
3. Shri Bhaskaran, IPS, DIG, TG</td><td>Tea Break</td></tr>
<tr><td></td><td>0930 - 1000 hrs</td><td>1000- 1030 hrs</td><td>1030 - 1110 hrs</td><td>1110 - 1130 hrs</td><td colspan="4">1130 - 1250 hrs</td><td>1250 - 1255 hrs</td><td>1255 -1330 hrs</td><td>1330 - 1500 hrs</td><td>1500 - 1545 hrs</td><td>1545 - 1615 hrs</td><td>1615 - 1625 hrs</td><td colspan="3">1625 - 1705 hrs</td><td>1705 hrs</td></tr>
<tr><td>18.03.2026 (Wednesday)</td><td>IT initiatives by SVPNPA

Shri Paramesh, Cyber X</td><td>Tech Initiatives in Goa

Shri Rahul Gupta, IPS, Goa</td><td>Challenges in technology implementation in policing & its experiences

Shri Senthil Avoodai Krishna Raj S, IPS, DIG, CISF</td><td>Tea Break</td><td colspan="3">Panel Discussion on Drone Technology

Basics of Drone Flight

Shri Harsh Panchal, Asst. Prof., NFSU

How to choose right techniques for Anti Drones

Shri Utkarsh, 2IC, ACDE Drone Warfare School Gwalior

Experience in local Law Enforcement

Shri Deepak Pareek, IPS, SP, ATS, Mohali</td><td>bio break</td><td>Panel Discussion on Drone Technology</td><td>LUNCH</td><td>Best Practices & Expereience Sharing in Maharashtra Police

(Online)

Shri Milind Bharambe, IPS, Commissioner of Police, Navi Mumbai, Maharashtra.</td><td>Tech Initiatives in Kerala

(Online)

Shri Ankit Ashokan, IPS, SP, KL</td><td>Tea Break</td><td colspan="3">Cyber Auditor

Dr. Rajesh Kumar Pal, Founder & CEO, Mobisec Technologies</td><td>Valediction</td></tr>
</table>

PART - I

Key Outcomes of the Workshop

Key Outcomes of the Workshop

1.1 Field-Tested Policing Technologies — A Compendium of Solutions Adopted by States, CPOs and CAPFs

One of the most important outputs of the workshop was the structured compilation of apps, tools and technology products being used by various police organisations. Inputs were collected from participating officers through a prescribed format covering the name of the tool, user agency, policing problem addressed, methodology adopted, product origin, cost model and perceived effectiveness.

The objective of this compendium is not merely to list technology products, but to identify solutions that have already been tested or used in real policing environments. This makes the compilation useful for replication, adaptation and informed procurement by other police organisations.

Methodology Adopted for the Compilation

The methodology followed for the compendium was based on peer learning and field validation. Participating officers were requested to share details of tools actually being used by their organisations, rather than products promoted only by vendors. The information was organised under broad policing categories such as cybercrime detection, investigation and station house management, citizen services, operations and intelligence, law and order, crime detection, traffic management and immigration-related policing.

For each tool or product, the following factors were captured:

Sl. No.	Factor	Description
1	User agency	State Police, CPO, CAPF or unit using the tool
2	Methodology / utility	Problem addressed and operational use of the tool
3	Product origin	In-house, MHA/Central, vendor-based or hybrid
4	Cost model	Free, subscription, one-time cost, AMC, fixed cost or not specified
5	Perceived effectiveness	High, medium, low, relevant or not specified, as reported by the user agency

This approach makes the compendium a practical field-oriented reference rather than a generic technology catalogue.

Category I: Cybercrime Detection

Cybercrime detection tools reported by participating agencies mainly support OSINT, social media monitoring, mobile forensics, CDR/IPDR analysis, cryptocurrency tracing, digital evidence imaging, password recovery and cyber patrolling.

Sl. No.	Tool / Product	User Agency	Methodology / Utility	Cost Model	Perceived Effectiveness
1	SpotTheScam	Goa Police	AI-based scam and fraud detection; cyber patrolling	Free / In-house	Medium
2	Cyber Patrolling Tool	Goa Police	Searches social media and suspicious APK files for fraud indicators	Free / In-house	Medium
3	PC3000 Pro	Maharashtra Police	Password recovery and forensic data extraction	One-time / Vendor	High
4	Ditto DX Forensic Field Tool	Maharashtra Police	Data imaging and cloning	One-time / Vendor	High
5	iCube CDR Solution	Maharashtra Police	CDR analysis with hash support	One-time / Vendor	High
6	Social Media Monitoring Tools	CRPF, Bijapur	Tracks radicalisation trends and misinformation	Subscription / Vendor	High
7	NCRB Portals / Samanvaya / Sahayog	Karnataka Police	Cybercrime coordination and data sharing	Free / MHA-Central	High / Medium
8	C-Trace / Daksh / Khoj	Delhi Police	CDR, IPDR and OSINT analysis	Subscription / Vendor	High
9	UFED / Oxygen / FTK / Autopsy	Delhi Police Crime Branch	Mobile and digital forensic examination	Subscription / Vendor	High
10	Chainalysis / Arkham Intelligence	Delhi Police Crime Branch	Cryptocurrency tracing and blockchain intelligence	Subscription / Vendor	High
11	ATOLA / FTK / Falcon / Write Blocker	Telangana Police / Warangal	Forensic imaging, disk analysis and evidence preservation	Free / In-house as reported	Medium

Key Outcomes:

These tools enhance cybercrime investigation by improving digital evidence recovery, mobile forensic extraction, cryptocurrency tracing, suspect identification, cyber patrolling and social media monitoring. They also support early identification of cyber fraud networks, mule accounts, phishing infrastructure and online radicalisation patterns.

Category II: Station House Management / Investigation

Tools under this category support police station digitisation, investigation workflows, evidence management, beat information, personnel systems, jail release monitoring and CDR/IPDR-based investigation.

Sl. No.	Tool / Product	User Agency	Methodology / Utility	Cost Model	Perceived Effectiveness
1	Deep Trace	Goa Police	Intelligence aggregation using vehicle, address and suspect parameters	Subscription / Vendor	High
2	i9 CDR Analyzer	Mizoram Police	CDR analysis and tower location support	Subscription / Vendor	High
3	JK Digital E-Library	J&K Police	Legal and investigation reference portal	Fixed Cost	Relevant
4	GTAMS	J&K CID	Monitoring of bailed-out persons	Fixed Cost	Relevant
5	CCTV Surveillance System	J&K Police	Police station and police post monitoring	Fixed Cost	Relevant
6	CCTNS CAS	J&K Police	FIR and police station digital workflow	Central / NCRB	Relevant
7	SAMBHAV / CLMS / SELO Inventory	CRPF, Bijapur	Personnel, material and canteen management	Free / In-house	High
8	HRMS / IMS / VMS	SSB	Personnel, inventory and vehicle management	MHA / Central	Not specified
9	NATGRID / Police IT / FLMS	Karnataka Police	Accused, suspect, evidence and department data management	Free / In-house / Vendor	High
10	CCTNS 2.0	Telangana Police	Customised police station workflow and investigation support	AMC / Hybrid	High
11	E-Sangrahan / M-Power	CISF ASG Kannur	Collection of applications for unit administration	Free / In-house	High

Sl. No.	Tool / Product	User Agency	Methodology / Utility	Cost Model	Perceived Effectiveness
12	E-Chitta / E-Malkhana / E-Beat Book	Delhi Police	Duty roster, property management and beat intelligence	Free / In-house	High
13	e-Petty	Telangana Police	Mobile-based petty offence enforcement	Free / In-house	Medium
14	JRMS / HRMS / CTrace / Verify 24x7	Telangana Police	Jail release monitoring, HR management, CDR and offender search	Free / Subscription	Medium
15	IPMCAP	Telangana Police	Patrol monitoring, crime mapping and accident analytics	In-house	Medium
16	eDAR	Telangana Police	Digital accident reporting integrated with police, transport, health and highways	Free / Central	Medium
17	ICJS / Cri-MAC / eSakshya	Multiple agencies	Criminal justice data exchange and digital evidence management	Free / Central	Medium

Key Outcomes:

These platforms improve the efficiency of police station functioning, reduce manual records, strengthen evidence management, support investigation workflows and improve coordination with courts, prisons, prosecution and forensic agencies.

Category III: Citizen Services

Citizen service tools aim to reduce the need for physical visits to police stations and improve transparency through online reporting, verification, grievance submission, emergency response and access to police services.

Sl. No.	Tool / Product	User Agency	Methodology / Utility	Cost Model	Perceived Effectiveness
1	Tenant Verification / 1930 Cloud	Goa Police	Digital identity and antecedent verification; cyber helpline support	Subscription / Vendor	High
2	DAKSH / Unch Bharai / Bharosa Cell / Abhaya	Maharashtra Police	Reporting, youth skilling, senior citizen and women support, travel safety	Not specified	Not specified
3	JKeCOP / J&K e-Services Portal	J&K Police	Online citizen services and verification	NCRB + Local customisation	Low
4	Madadgaar Helpline	CRPF	24x7 helpdesk for citizens in J&K	Free / In-house	High
5	Anubhav QR Code	Chhattisgarh Police	Citizen feedback on police station services	Free / In-house	Medium
6	KSP App / Safety Islands / BTP Astram Lock	Karnataka Police	Lost report, drug report, traffic updates and public safety	Free / Subscription	High / Medium
7	Lost Report / MV Theft / E-FIR / Missing Person / PCC	Delhi Police	Online reporting and certificate services	Free / In-house	High
8	Citizen Portal	Telangana Police	Online petitions, FIR copy, missing persons and arrest reports	Free / In-house	Medium
9	Meeseva	Telangana Police	Digital certificates, permissions and police services	Free / In-house	Medium
10	Prajavani	Telangana Police	Public grievance redressal	Free / In-house	Medium
11	CEIR	Telangana Police	Blocking and recovery support for stolen mobile phones	Free / Central	Medium
12	Hawkeye / Hawkeye Ultra	Telangana Police	SOS, citizen reporting and community policing	Free / Hybrid	High / Medium

Key Outcomes:

Citizen service platforms improve accessibility, transparency and public trust. They reduce physical interface with police stations, enable faster grievance registration and support women safety, senior citizen services, emergency reporting and public feedback.

Category IV: Operations / Intelligence

Operational and intelligence tools use GIS, satellite communication, drone surveillance, intelligence databases, social media monitoring and secure communication systems to improve field-level situational awareness.

Sl. No.	Tool / Product	User Agency	Methodology / Utility	Cost Model	Perceived Effectiveness
1	Deep Trace	Goa Police	Target intelligence generation	Not specified	Not specified
2	NATGRID	Maharashtra / Mizoram / Delhi / Telangana / Karnataka	Multi-database intelligence integration	Free / MHA-Central	High / Medium
3	C-DAT	Telangana SIB	CDR, IPDR and PCAP analysis	In-house	Not specified
4	GIS / Alpine	ITBP	Terrain analysis, offline tracking and operational planning	Subscription / In-house	Medium
5	UAV / Netral / Bhushakti	CRPF, Bijapur	Aerial reconnaissance and map-based intelligence	One-time / Central	High
6	POLNET / ISPW Grid	DCPW, MHA	Satellite-based secure police communication	One-time / Subscription	High / Medium
7	STAR GIS	ITBP	Target area analysis, patrol route marking and satellite imagery	In-house	High
8	SPECS	NTRO	GIS-based silent patrolling and real-time tracking	One-time / In-house	High
9	Unocross	Telangana Police	CDR and tower dump request management	Free / In-house	Medium
10	DOPAMS	Telangana Police	Drug offender monitoring and NDPS intelligence	Free / In-house	Medium
11	CyCAPS	Telangana Police	Cybercrime accused profiling and national linkage	Free / In-house	Medium
12	Vatsalya / Darpan / Talash	Telangana Police	Child tracking, missing persons and offender search	Free / In-house / Central	Medium

Key Outcomes:

These tools strengthen intelligence-led operations, improve terrain and patrol planning, support secure communications in remote areas and assist in tracking organised crime, cybercrime, drug networks and missing persons.

Category V: Law & Order / Crime Detection

Tools in this category support crime prevention, field verification, facial recognition, offender identification, patrol deployment, CCTV analytics and command-and-control functions.

Sl. No.	Tool / Product	User Agency	Methodology / Utility	Cost Model	Perceived Effectiveness
1	Facial Recognition System	J&K Police	AI-enabled suspect identification using CCTV and legacy data	Fixed Cost / Vendor	Not specified
2	UT-wide CCTV Surveillance	J&K Police	Integrated command and control for real-time monitoring	Fixed Cost / Vendor	Not specified
3	NATGRID / MCCTNS / Drones / Mobile Command Centre	Karnataka Police	Accused management, data analysis, bandobast and surveillance	Mixed	High
4	TSCOP	Telangana Police	Frontline mobile application for crime prevention and investigation	AMC / Hybrid	High
5	IPMS / IMCAP	Telangana Police	Crime, accident and patrol analytics	AMC / Hybrid	High
6	CCTNS / ICJS	Delhi Police	Crime and criminal record management	Free / Central	High
7	CIS / Enterprise Search	Telangana Police	Offender, jail release, missing person and vehicle search	Free / In-house	Medium
8	Fingerprint Mobile App	Telangana Police	Fingerprint collection and accused detection	Free / In-house	Medium
9	Anubhav QR Code	Chhattisgarh Police	Citizen feedback on police services	Free / In-house	High

Key Outcomes:

These tools improve field-level access to crime data, support offender identification, strengthen command-and-control systems and improve law and order deployment through analytics, surveillance and real-time information access.

Category VI: Traffic Management

Traffic management tools use AI cameras, e-challan systems, citizen reporting apps, body-worn cameras and drones for evidence-based enforcement and road safety.

Sl. No.	Tool / Product	User Agency	Methodology / Utility	Cost Model	Perceived Effectiveness
1	AI Camera	Karnataka Police	Traffic violation detection and signal management	One-time / Vendor	High
2	BTP Astram	Karnataka Police	Traffic updates and public safety	Subscription / Vendor	High
3	Body-Worn Cameras	Karnataka Police	Transparency in traffic enforcement	One-time / Vendor	High
4	Drones	Karnataka Police	Traffic monitoring and enforcement support	One-time / Vendor	High
5	Delhi Traffic Police App / Traffic Prahari	Delhi Police	Citizen reporting of traffic violations through photos/ videos	Free / In-house	High
6	e-Ticket / e-Challan	Telangana Police	Cashless, contactless, evidence-based traffic enforcement	Free / In-house	Medium

Key Outcomes:

Traffic technology improves evidence-based enforcement, reduces cash handling, enhances transparency, improves traffic discipline and supports citizen participation in traffic regulation.

Category VII: Immigration / Foreigners

Tools in this category support immigration verification, foreigner tracking, visa services, entry-exit monitoring and police verification.

Sl. No.	Tool / Product	User Agency	Methodology / Utility	Cost Model	Perceived Effectiveness
1	Maharashtra State Police Module	Maharashtra Police	Immigration and foreigner-related policing	Free / Central	High
2	NATGRID	Karnataka Police	Immigration and foreigner data access	Free / Central	High
3	Delhi Police Module by NIC & BOI	Delhi Police	Foreigner entry, exit and stay verification	Free / Central	High
4	Verify 24x7	Telangana Police	National offender search using name, age, address and mobile number	Free / Central	Medium
5	IVFRT	Telangana Police	Visa extension, residential permit, departure and police clearance services	Free / Central	Medium

Key Outcomes:

These systems support national security, foreigner verification, immigration-related investigation and integration with central databases.

Overall synthesis of the Technology Compendium:

Product origin:

Sl. No.	Product Origin	Examples	Observation
1	In-house	SpotTheScam, E-Malkhana, TSCOP, CyCAPS, Hawkeye	Low-cost, adaptable and suitable for replication
2	MHA / Central	NATGRID, CCTNS, ICJS, CEIR, IVFRT	Scalable and nationally standardised
3	Vendor-based	PC3000, Oxygen, UFED, Chainalysis, AI Cameras	High capability but may involve recurring cost
4	Hybrid	CCTNS 2.0 Telangana, Hawkeye Ultra	Combines police domain knowledge with external technical development

Cost model:

Sl. No.	Cost Type	Common Domains	Remarks
1	Free / Zero Cost	Central portals, in-house apps, citizen services	Best suited for immediate replication
2	Subscription	OSINT, forensic tools, CDR/IPDR tools, GIS	Requires recurring budget support
3	One-time Cost	Hardware, drones, forensic devices, CCTV	Requires maintenance and upgrade planning
4	AMC / Fixed Cost	Large platforms and surveillance systems	Needs lifecycle management
5	Not specified	Some State-specific tools	Requires follow-up before replication

Perceived effectiveness:

Sl. No.	Effectiveness Level	Common Tool Types	Interpretation
1	High	NATGRID, CCTNS, E-Malkhana, forensic tools, citizen portals, traffic apps	Strong user confidence and replication potential
2	Medium	Many in-house AI, CDR, citizen and cyber tools	Useful but may require refinement or scaling support
3	Low	Some under-redevelopment citizen platforms	Requires redesign or user feedback
4	Not specified	Some agency-specific entries	Needs further validation before adoption

1.2 Summary Outcomes of the Panel Discussions:

The workshop included two major panel discussions: Artificial Intelligence in Investigation – Field-Level Applications and Drone Technology. These discussions were among the most significant components of the workshop because they addressed emerging technologies that are directly relevant to investigation, surveillance, internal security and operational preparedness.

1.2.1 Artificial Intelligence in Investigation – Field-Level Applications

The panel discussion on AI in investigation was moderated by **Shri Ajit Pratap Singh, IPS, DD (IT-2), SVP NPA.** The panellists included **Ms. Mallika Garg, IPS, SP, Andhra Pradesh; Shri Amit Kumar, IPS, Commandant, State Reserve Police, Uttar Pradesh; Shri K. Pratap SivaKishore, IPS, SP, Andhra Pradesh; and Shri Bhaskaran, IPS, DIG, Telangana Police.** A related session by **Shri Milind Bharambe, IPS, Commissioner of Police, Navi Mumbai,** further enriched the discussion on AI-assisted investigation.

The discussion highlighted that AI can significantly improve the quality, speed and consistency of investigations. AI-based systems are being used for FIR analysis, legal section identification, chargesheet support, evidence evaluation, CCTV analysis, facial recognition, predictive policing, tower dump analysis, CDR/IPDR interpretation and investigation workflow support.

The key outcome was the recognition that AI should function as an investigation assistant or force multiplier, not as a substitute for human judgment. Police officers must retain final decision-making authority, especially in matters relating to evidence appreciation, chargesheet filing and prosecution. The panel also highlighted the importance of secure data infrastructure, data sovereignty, auditability, explainability and ethical use of AI.

Key Outcomes of the AI Panel:

- AI can reduce repetitive documentation and improve investigation quality.
- AI tools can support FIR analysis, legal section suggestion, evidence grading and compliance verification.
- Predictive policing can assist in hotspot identification and preventive deployment.
- Integrated AI ecosystems can improve link analysis and intelligence generation.
- Sovereign and secure AI models are preferable for sensitive police data.
- Human supervision and accountability must remain central.
- Deepfakes and AI-generated cyber threats require enhanced forensic preparedness.

Note: Detailed summary of each sessions are given on page no.

23 (Ms. Mallika Garg, IPS), 24 (Shri Amit Kumar, IPS), 25 (Shri K. Pratap SivaKishore, IPS), 26 (Shri Bhaskaran, IPS) and 28 (Shri Milind Bharambe).

1.2.2 Drone Technology and Counter-Drone Preparedness:

The panel discussion on Drone Technology was moderated by **Shri Ilango R, IPS, Assistant Director, SVP NPA / Workshop Director.** The panellists included **Shri Harsh Panchal, Assistant Professor, NFSU; Shri Utkarsh, 2IC, ACDE Drone Warfare School, Gwalior; and Shri Deepak Pareek, IPS, SP, ATS, Mohali.** A related session by **Shri Ankit Ashokan, IPS, SP, Kerala Police,** highlighted practical technology initiatives including anti-drone applications.

The discussion covered drone basics, drone classifications, drone payloads, telemetry, forensic value of drone components, anti-drone techniques and the operational experience of Punjab Police in countering cross-border drone threats. Punjab Police's **Baazak** anti-drone system and Kerala Police's **Eagle Eye** anti-drone initiative were important practical examples.

The key outcome was that drones must be understood both as policing assets and as emerging security threats. Drones can assist in surveillance, crowd management, border monitoring, disaster response and public safety. At the same time, hostile drones pose serious risks in border areas, prisons, VIP security zones, airports and critical infrastructure.

Key Outcomes of the Drone Technology Panel:

- Drones are increasingly important for surveillance, public safety and operational policing.
- Drone controllers, memory cards, cloud accounts, flight logs and telemetry can serve as forensic evidence.
- Counter-drone response must follow a layered approach: detect, track, identify, assess and neutralise.
- Punjab Police's experience demonstrates the need for coordinated police, BSF and Army response to cross-border drone threats.
- Counter-drone systems require AI-based classification, multi-sensor fusion and improved jamming or cyber takeover capabilities.
- State Police organisations require SOPs for drone deployment, neutralisation, recovery and forensic examination.
- Drone-related training should be integrated with cyber forensics and field operations training.

Note: Further details of the above sessions are given on page no

page no. 30 (Shri Harsh Panchal), page no. 34 (Shri Utkarsh), page no. 35 (Shri Deepak Pareek, IPS) and page no. 38 (Shri Ankit Ashokan, IPS).

Recommendations Emerging from the Key Outcomes

1. A national repository of field-tested policing technologies may be developed and periodically updated.
2. Tools may be classified by user agency, methodology, cost model, product origin and perceived effectiveness.
3. Free, high-effectiveness and in-house tools may be prioritised for inter-state replication.
4. Paid vendor products may be evaluated through structured user feedback and cost-benefit analysis before wider adoption.
5. AI investigation tools should be developed within secure and preferably government-controlled infrastructure.
6. Counter-drone SOPs should be developed for border districts, airports, prisons, VIP security and critical infrastructure.
7. Police officers should be trained in AI-assisted investigation, drone forensics, digital evidence handling and technology procurement evaluation.
8. The compendium should be treated as a living ready reckoner and updated with new tools, user feedback, operational outcomes and replication status.

PART - II

Brief Summary of Sessions

Brief Summary of Sessions

Technology adoption in policing is most meaningful when it is connected with real field requirements, operational challenges, and measurable outcomes. The technical sessions of the workshop brought this perspective into focus by presenting a wide range of technologies, platforms, and implementation experiences relevant to investigation, internal security, communication, cybercrime detection, citizen services, aviation security, and digital forensics. Rather than treating technology as a standalone solution, the sessions emphasized its role as an enabler that must support police processes, improve decision-making, reduce manual workload, and strengthen coordination among agencies.

The sessions covered important themes such as opportunities and challenges in technology adoption, DRDO's association with police and CAPFs, NATGRID-based data sharing, CCTNS and ICJS integration, mule account identification, cybercrime investigation, POLNET and public protection communication systems, aviation security, IT initiatives of SVP NPA, problem-driven innovation in policing, implementation challenges, and cyber auditing. These discussions helped participants understand both the potential and the limitations of technology in real policing conditions. A recurring message across the sessions was that successful implementation depends not only on advanced tools, but also on user acceptance, data quality, training, system integration, cybersecurity, and continuous human oversight.

The sessions also highlighted practical models and best practices from different organisations, including AI-enabled investigation support, secure communication systems, national crime data integration, cyber forensic tools, citizen-centric applications, predictive policing models, and cybersecurity auditing mechanisms. Together, they created a rich learning environment where participants could compare approaches, identify scalable solutions, and reflect on how technology can be adapted to local needs. Overall, this part brings together the key learning outcomes of the workshop and reinforces the need for thoughtful, secure, user-friendly, and field-oriented technology adoption in modern policing.

2.1 Technology in Policing – Opportunities, Challenges and Limitations

Presenter's Details:
Shri Vinit Dev Wankade, IPS
CMD, Tamil Nadu Police Housing Corporation Ltd.

Executive Summary:

The session examined the evolving integration of technology in modern policing, highlighting both its transformative potential and inherent limitations. While tools such as Artificial Intelligence (AI), Machine Learning (ML), and advanced surveillance systems have enhanced efficiency in crime detection, monitoring, and administration, their success depends on thoughtful, need-based implementation. The discussion emphasized that technology must complement— not replace—core policing functions, and its effectiveness is contingent on user acceptance, process integration, and data reliability. Key challenges identified included misaligned adoption, resistance among personnel, data integrity concerns, and over-

dependence on vendor-driven solutions.

Key Highlights:

- **Transformation of Policing:**
  - Shift towards data-driven and technology- enabled policing systems.
  - Enhanced capabilities in crime detection, surveillance, and administrative efficiency.
- **Challenges in Technology Adoption:**
  - Adoption often driven by visibility or vendor influence rather than operational need.
  - Risk of misalignment between technological solutions and ground realities.
- **Need-Based and Outcome-Oriented Implementation:**
  - Systems must be aligned with actual field requirements.
  - Focus should be on measurable outcomes rather than mere deployment.
- **Human Factors and Resistance:**
  - Resistance observed across ranks due to increased workload and monitoring.
  - Duplication of processes reduces efficiency and acceptance.

- **User-Centric Design:**
  - Systems must be intuitive and reduce operational burden.
  - Greater acceptance when designed around user needs and workflows.
- **Ownership and Governance:**
  - Police personnel must retain ownership of technological systems.
  - Domain experts should guide implementation and customization.
- **Process-Centric Integration:**
  - Technology should integrate seamlessly into existing policing processes.
  - Should support, not disrupt, operational workflows.
- **Limitations of Technology:**
  - Technological tools are probabilistic, not infallible.
  - Require human oversight and validation.
- **Data Integrity and Reliability:**
  - Accuracy of input data is critical for reliable outputs.
  - Poor data quality can lead to flawed analysis and investigations.
- **System Robustness:**
  - Systems must incorporate validation checks, redundancy, and audit mechanisms.
  - Preparedness for failures is essential for reliability.

Key Outcomes:

- Recognition that **technology is an enabler, not a substitute for policing.**
- Emphasis on **need-based, field-oriented technology adoption.**
- Improved understanding of **human factors influencing technology acceptance.**
- Strengthened focus on **data quality and system reliability.**
- Reinforcement of **process-driven implementation over tool-driven deployment.**
- Greater awareness of the need for **balanced integration of human judgment and technology.**

2. 2 DRDO's Association with CAPFs, Police & BPR&D and Technologies for Internal Security

Presenter's Details:
Shri A. Sangita Rao Achary, Director,
DRDO – Directorate of Low Intensity Conflicts (DLIC)

Executive Summary:

The session delivered a comprehensive overview of the Defence Research and Development Organisation (DRDO)'s role in strengthening internal security through advanced, indigenous technologies and structured collaboration with the Ministry of Home Affairs (MHA), Central Armed Police Forces (CAPFs), State Police, and BPR&D. It highlighted DRDO's model of developing cutting- edge systems and transferring them to industry for large-scale deployment. The discussion covered a wide spectrum of technologies including small arms, anti- drone systems, surveillance tools, IED detection solutions, communication systems, and non-lethal crowd control equipment. Overall, the session emphasized enhanced operational capability, improved personnel safety, and preparedness against evolving security threats.

Highlights:

- **Institutional Collaboration Framework:**
  - DRDO works in close coordination with MHA, CAPFs, State Police, and BPR&D.
  - Directorate of Law Enforcement Interface Cell (DLIC) acts as a bridge between developers and end users.
  - Supported by Apex Council and Technology Council for strategic oversight.
- **Technology Development & Transfer Model:**
  - DRDO develops advanced technologies and transfers them to industry via ToT.
  - Ensures indigenous production, scalability, and cost efficiency.
- **Small Arms and Ammunition:**
  - Induction of machine pistols, LMGs, CQB systems, JVPC, and INSAS rifles.
  - Advanced grenade systems (MMHG, UBGL) enhance combat capabilities.
- **Anti-Drone Systems:**
  - Multi-layered architecture: Detection (radar, RF, acoustic).
  - Identification (EO/IR), Neutralization (soft & hard kill).

- Includes RF jammers, GNSS spoofing, laser weapons, and microwave systems.
- Portable and field-deployable solutions available.

- **Surveillance & Intelligence Systems:**
  - Facial Recognition Systems (FRS) and AI-based crowd behaviour analysis.
  - Border Surveillance System (BOSS) for long-range monitoring.
  - Enables predictive policing and real-time situational awareness.
- **IED Detection & Neutralization:**
  - Ground Penetrating Radar (GPR), bomb disposal robots, IED jammers.
  - Explosive trace detection and drone-based detection (under development).
- **Crowd Control & Protection:**
  - Non-lethal systems: chilli grenades, plastic bullets, dazzlers.
  - Protective gear: riot suits, blast suits, bulletproof jackets and helmets.
- **Communication Systems:**
  - Software Defined Radios (SDR), digital handheld devices.
  - Secure long-range communication for operations in denied environments.
- **Procurement Mechanism:**
  - Technologies procured via LTE, open tenders, and direct procurement.
  - CAPFs and State Police actively participate in trials and adoption.

Key Outcomes:

- Strengthened integration between defence R&D and internal security agencies.
- Enhanced operational effectiveness in counter-insurgency, border security, and urban policing.
- Improved personnel safety through advanced protective and non-lethal systems.
- Increased situational awareness and decision-making capability using AI- driven surveillance tools.
- Boost to indigenous manufacturing and self-reliance through technology transfer.
- Greater readiness to counter emerging threats, particularly drones and IEDs.
- Improved communication resilience in remote and infrastructure-denied environments.

2. 3 NATGRID Database for Policing – Data Sharing with Law Enforcement Agencies (LEAs)

Presenter's Details:
Shri B. Praveen
Joint Secretary, NATGRID

Executive Summary:

The session provided a detailed overview of the National Intelligence Grid (NATGRID) as a critical enabler of data-driven policing and national security. It highlighted NATGRID's role in integrating multiple government databases into a unified analytical platform, enabling real-time access to intelligence for authorized agencies. By leveraging advanced graph-based analytics, artificial intelligence, and secure data-sharing mechanisms, NATGRID enhances investigation, counter-terrorism efforts, and inter-agency coordination. The session also addressed operational challenges such as limited field-level access and underutilization, while emphasizing the need for capacity building and wider adoption.

Specifications (Key Highlights – Refined)

- Integrates data from ~28 databases across financial, travel, and identity domains, connecting 47 user agencies and 14 data providers.
- Uses graph-based architecture (nodes and edges) to establish relationships and enable multi-hop analysis of entities.
- **GANDIVA (Query-Based Intelligence System):**
  - Enables search across 200+ crore images.
  - Supports geo-spatial and time-series analysis.
  - Provides CDR analysis and profile enrichment.
  - Includes collaboration tools such as alerts and watchlists.
- **SUDARSHAN (OSINT Platform):**
  - Monitors social media and open-source platforms.
  - Uses AI/LLMs for summarization and analysis.
  - Supports OCR and multilingual translation.
  - Performs audio, video, and image analytics, including dark web profiling.
- Employs advanced analytics such as Multi-Dimensional Entity Resolution (MDER) for identity matching.

- Uses graph algorithms for link prediction, node classification, and behavioural pattern analysis.
- Implements a secure, role-based access hierarchy (Designated, Approving, Supervisory, Authorized, Nodal Officers).
- Ensures data security through multi-layer authentication, audit trails, and secure VDI-based access.
- Supports real-time intelligence generation, inter-agency collaboration, and reduction of manual data dependency.

Key Outcomes:

- Strengthened intelligence-led policing and data-driven investigations.
- Enhanced real-time access to integrated multi-source data.
- Improved inter-agency coordination and information sharing.
- Increased efficiency and accuracy in investigations.
- Strengthened national security and counter-terrorism capabilities.
- Emphasized need for capacity building and wider system adoption.
- Improved ability to detect hidden networks and behavioural patterns.

2. 4 Artificial Intelligence in Investigation – Field-Level Applications

Presenter's Details:
Ms. Mallika Garg, IPS,
Superintendent of Police, Andhra Pradesh

Executive Summary:

The session highlighted how Andhra Pradesh Police is using an AI-based "Investigation Copilot" to tackle challenges like information overload, legal complexity, and delays in investigations. The system acts as an intelligent assistant, supporting officers from FIR registration to chargesheet preparation by automating documentation, suggesting legal sections, and guiding evidence collection. It also enables smart complaint analysis, real-time surveillance through CCTV and face recognition, and efficient handling of digital evidence like CDR/IPDR. Additionally, integrated media and social intelligence tools help in tracking trends and linking cases. Overall, the session demonstrated that AI enhances investigation quality, speeds up decision-making, and ensures consistency, while keeping human officers in control.

Key Highlights:

2. 4. 1 From Reactive to Proactive Policing

Presenter's Details:
Shri Amit Kumar, IPS,
Commandant, State Reserve Police, Uttar Pradesh

Executive Summary:

This session focused on the shift from reactive to proactive policing using AI-driven predictive models. By analyzing historical crime data, AI helps predict potential crime locations, timings, and suspects, enabling preventive actions like targeted patrolling and better resource deployment. The approach is built on three pillars: place-based policing (identifying hotspots), person-based policing (tracking repeat offenders), and administrative efficiency (automating police tasks). The session also highlighted challenges such as poor data quality and the "black box" nature of AI, emphasizing the need for transparent "glass box" systems. It stressed the importance of privacy protection while handling sensitive data. Overall, AI was presented as a powerful tool to support proactive policing while ensuring human oversight and accountability.

Key Highlights:

- AI enables early identification of potential crime areas and risks.
- Improves preventive policing and reduces dependency on post-crime response.
- Enhances efficiency in deployment of police personnel and resources.
- Helps in monitoring repeat offenders more effectively.
- Reduces workload of officers through automation of routine tasks.
- Builds trust through transparent and explainable AI systems.
- Ensures balance between law enforcement needs and citizen privacy.

2. 4. 2 AI as an "Ironman Suit" for Police

Presenter's Details:
Shri K Pratap SivaKishore, IPS,
SP, Andhra Pradesh

Executive Summary:

This session presented AI as an "Ironman Suit" that enhances the capabilities of police officers rather than replacing them. It addressed key challenges such as legal complexity, language barriers, trial confusion, and heavy documentation by introducing an AI-driven framework led by DHARMA, supported by systems like VEDA, GARUDA, and 360° crime scene technology. These tools assist in complaint analysis, legal guidance, surveillance, evidence handling, and trial preparation, significantly improving investigation quality and efficiency. The session highlighted real-world impact, including improved documentation and higher conviction outcomes. It also emphasized ethical use, transparency, and the need for continuous human supervision. AI was presented as a powerful force multiplier that supports smarter, faster, and more effective policing.

Key Highlights:

2. 4. 3 AI Ecosystem in Telangana Police

Presenter's Details:
Shri Bhaskaran, IPS,
(DIG, Telangana)

Executive Summary:

The session explained how Telangana Police has built a large-scale, integrated AI ecosystem to support investigations and decision-making. Platforms like Infinity, Agentic AI, Playground, and Vishleshan enable real-time insights, link analysis, and seamless access to multiple datasets, helping officers uncover hidden connections in complex cases. A centralized Data Lake further strengthens this system by bringing together FIRs, intelligence inputs, and suspect data in one place. Advanced tools such as Crime Copilot, CDAT AI, tower dump analysis, and image enhancement significantly improve speed and accuracy of investigations. The session highlighted that strong data integration is key to making AI effective in policing. Overall, it showed how a well-connected AI ecosystem can enhance efficiency, accuracy, and timely decision-making in modern policing.

Key Highlights:

Panel Discussion: Challenges and Future of AI in Policing

Executive Summary:

The panel discussion brought together senior officers to examine the challenges and future of AI in policing, focusing on issues like data security, infrastructure, and ethical use. A key concern was data sovereignty, with emphasis on keeping sensitive police data within secure government systems and preferably on intranet networks. A major highlight was the growing threat of deepfakes, where AI-generated fake videos and images are increasingly used in crimes, making detection a critical challenge for law enforcement. The discussion also noted the high cost and infrastructure needs of AI, especially for smaller states. While advanced tools like AI-based surveillance and drones are improving policing, officers stressed that AI must only assist and not replace human judgment. Overall, the session emphasized responsible, transparent, and secure use of AI while maintaining accountability.

Key Highlights:

Data Sovereignty & Security:

- Police data must remain within secure government infrastructure.
- Prefer Intranet-based systems over public internet.
- Prevents data leaks and unauthorized access.

Deep fake & Cyber Threats:

- Rising misuse of deep fake videos/images in crimes.
- Requires advanced AI detection tools.
- Major challenge for cyber forensics.

Use of Advanced AI Models (e.g., YOLO):

- Real-time object detection for surveillance.
- Used in crowd monitoring, vehicle tracking.

AI-Enabled Drones:

- Used for VIP security and large crowd monitoring.
- Provides real-time intelligence from field.

Over-Reliance on AI – Major Concern:

- AI should assist, not replace officers.
- Cannot independently file charge sheets.
- Human judgment must remain final.

2. 4. 4 Best Practices & Experience Sharing in Maharashtra Police

Presenter's Details:
Shri Milind Bharambe, IPS,
Commissioner of Police, Navi Mumbai, Maharashtra.

Executive Summary:

The session focused on the best practices and technology initiatives implemented by Maharashtra Police, particularly the use of Artificial Intelligence in policing and investigation processes. The presentation highlighted "Unvasion AI," a sovereign AI solution developed in-house by Navi Mumbai Police to support investigation, charge sheet analysis, evidence evaluation, and decision support for investigating officers. The initiative was designed to improve investigation quality, reduce procedural lapses, strengthen evidence assessment, and enhance fair conviction outcomes.

The AI system integrates BNS, BNSS, BSA, police manuals, SOPs, Supreme Court and High Court case laws, and multilingual OCR capabilities for Marathi and English documentation. The model supports both standardized investigations and dynamic, complex investigations by providing automated analysis, investigation guidance, compliance verification, evidence grading, and actionable recommendations.

Key Highlights:

- Maharashtra Police presented various technology initiatives including AI applications, CCTV and drone usage, citizen-centric services, social media applications, welfare initiatives, crowd measurement, and CCTV management.
- "Unvasion AI" was introduced as a sovereign AI solution for investigation support and charge sheet analysis in Navi Mumbai Police.
- **The AI system supports:**
  - Automated charge sheet analysis
  - Instant FIR analysis
  - Dynamic investigation guidance
  - Evidence evaluation and grading
  - Mandatory compliance verification
  - Investigation workflow support
- Maharashtra Police developed its own OCR model trained for handwritten Marathi documents with more than 600 hours of training.
- **The platform categorizes evidence into:**
  - Documentary evidence.

- Oral evidence.
- Digital evidence.
- Medical and forensic evidence.

- **The AI model evaluates:**
  - Admissibility and inadmissibility of evidence.
  - Contradictions and omissions.
  - Strength of evidence (strong, moderate, weak).
  - Mandatory procedural compliances.
- **The system provides actionable guidance to investigating officers, including:**
  - Missing investigation steps.
  - Pending compliances.
  - Required evidence collection.
  - Court submission readiness.
- **The application supports bilingual report generation in Marathi and English.**

Key Outcomes:

- Improved investigation quality through AI-assisted evidence appreciation and analysis.
- Reduction in investigation lacunae before charge sheet submission.
- Enhanced support for investigating officers handling multiple law and order responsibilities.
- Standardization of investigation workflows and procedural compliance verification.
- Faster identification of missing evidence, contradictions, and compliance gaps.
- Strengthened evidence-based investigation through evidence grading and admissibility analysis.
- Dynamic investigation planning for complex cases based on cumulative case inputs.
- Improved multilingual document processing capabilities for Marathi and English records.
- Development of a fully sovereign and secure AI ecosystem within Maharashtra Police.
- Focus on achieving fair conviction outcomes through scientifically guided investigation processes.

2. 5 Drone Technology and Counter-Drone Preparedness

2. 5. 1 Basics of Drone Flight

Presenter's Details:
Shri Harsh Panchal, NFSU

Executive Summary:

The session "Basics of Drone" presents a concise, forensic-oriented overview of Unmanned Aerial Vehicles (UAVs), covering their evolution, classification, system architecture, components, and investigative relevance. It frames drones as strategically significant assets across civilian, commercial, and military domains.

Starting from early unmanned concepts (1849), it moves to modern applications such as surveillance, logistics, and public displays, while highlighting cost asymmetry in warfare, where low-cost drones can counter high-value defense systems.

Drones are defined as part of an Unmanned Aircraft System (UAS)—comprising the UAV, ground control station, and communication link—and are classified by design with clear operational trade-offs.

The presenter also outlines core components and control systems, emphasizing that devices such as controllers, mobile apps, storage media, and cloud platforms serve as critical sources of digital and physical forensic evidence.

Overall, it establishes drones as multi-domain enablers in security, surveillance, logistics, and forensics, underscoring the need for technical understanding in both operations and investigations.

Fig: Types of Drones

Key Highlights:

1. Historical and Strategic Context:

- UAV concepts predate modern aviation (1849 aerial bombing example).
- Demonstrates early understanding of remote warfare capability.

2. Expanding Applications:

- Civilian: Photography, delivery, crowd monitoring, drone light shows.
- Military: ISR (Intelligence, Surveillance, Reconnaissance), combat, logistics.
- Emerging dual-use nature (civil + defense).

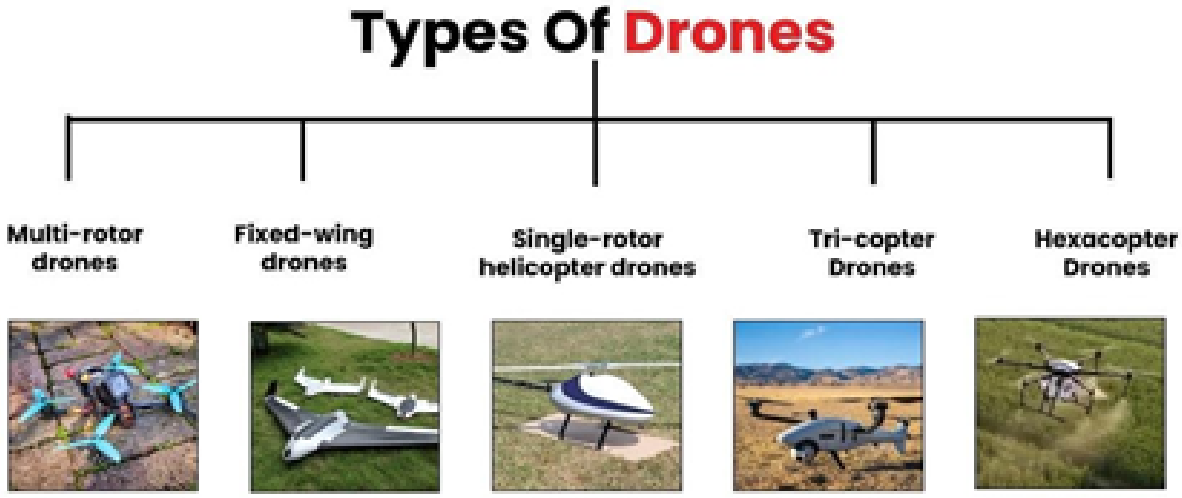
3. Cost Asymmetry in Warfare:

- Example: ~$20K drone vs ~$4M missile interception.
- Highlights economic disruption in defense strategy.

Fig: Military Drones

4. Drone System Architecture (UAS):

- **Three core elements:**
  - UAV (aircraft).
  - Ground Control Station.
  - Communication Link.
- Emphasizes system-level understanding over just the drone.



Each type has unique capabilities,
from hobby use to professional industry applications.

Fig: Drone classifications

5. Classification of Drones:

- Multi-rotor: stable, short endurance.
- Single-rotor: efficient, heavy payload.
- Fixed-wing: long range, no hovering.
- Hybrid: combines VTOL + endurance.
- Military drones: high endurance, combat-ready.

Fig: Drone Core Components

6. Core Components:

- Airframe, propulsion system, flight controller, payload.
- Subcomponents include ESCs, batteries, propellers, transmitters.

7. Payload Versatility:

- Cameras, sensors, logistics payloads, and weapon systems.
- Defines mission capability of the drone.

8. Control Systems & Data Sources:

- Remote controller, mobile apps, FPV systems.
- Store critical data: GPS logs, telemetry, media, credentials.

9. Forensic Significance:

- Every component (hardware + software) is an evidence source.
- Includes:
  - Flight logs.
  - Memory cards.
  - Cloud data.
  - Physical residues (DNA, fingerprints).

Takeaways:

1. Drones as Strategic Assets:

- Transitioned from experimental tools to core assets in defense, governance, and industry.

2. Need for Technical Literacy:

- Effective handling (operation or investigation) requires understanding:
  - System architecture.
  - Flight dynamics.
  - Data ecosystems.

3. Forensic and Security Relevance:

- Drones introduce new digital and physical evidence vectors.
- Law enforcement must adapt to UAV-specific investigation techniques.

4. Policy and Regulatory Importance:

- Growing usage necessitates strong regulatory frameworks (implied in document scope).

5. Operational Trade-offs Awareness:

- Each drone type presents clear trade-offs in endurance, payload, stability, and cost.

6. Emerging Threat Landscape:

- Low-cost drones create asymmetric threats, especially in defense and critical infrastructure.

7. Integration with Digital Ecosystems:

- **Modern drones are deeply integrated with:**
  - Mobile apps.
  - Cloud platforms.
  - Telemetry systems.

Fig: DGCA Airspace Map — Dynamic Platform

2. 5. 2 Choosing the Right Techniques for Anti-Drones

Presenter's Details:
Shri Utkarsh,
21C ACIDE Drone Warfare School

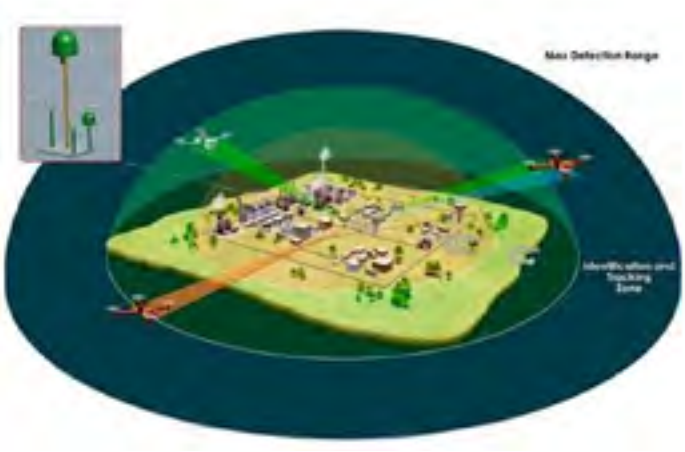
Executive Summary:

Effective anti-drone operations require a context-driven and multi-layered approach, where the selection of techniques depends on the nature of the threat, operational environment, and safety considerations. Rather than relying on a single method, law enforcement agencies must adopt a combination of detection, monitoring, and neutralization strategies while ensuring minimal risk to civilians and surrounding infrastructure.

Key Highlights:

- Technique selection is situation-dependent, based on threat type, location, and urgency.
- Anti-drone measures include:
  - Detection and monitoring systems.
  - Electronic countermeasures (signal disruption).
  - Physical neutralization methods.
- AI-enabled surveillance systems enhance detection and tracking capabilities.
- Emphasis on layered defense approach (detect → track → respond).
- Decision-making must consider:
  - Threat level.
  - Presence of payload.
  - Population density.
  - Risk of collateral damage.
- Operational response must balance effectiveness, safety, and legal constraints.

Key Outcomes:



- Improved ability to identify and respond to drone threats in real time.
- Enhanced situational awareness through integrated surveillance systems.
- Reduction in risks to civilians through controlled and appropriate response selection.
- Increased operational efficiency using multi-layered and adaptive techniques.
- Strengthened preparedness for diverse and evolving drone threats.

2. 5. 3 Experience in Local Law Enforcement

Presenter's Details:
Shri Deepak Pareek, IPS,
SP, ATS Mohali

Executive Summary:

The session focused on the practical experiences of Punjab Police in procuring and deploying anti-drone systems to address cross-border drone threats originating from Pakistan. The presentation highlighted the operational realities faced by Punjab Police, BSF, and the Army in managing drone-based smuggling and security threats along the international border.

Punjab Police introduced its vehicle-mounted portable anti-drone system named "Baazak," meaning "hawk eye" in Punjabi. Punjab Police became the first border state police in the country to directly engage hostile drones crossing the international border. The presentation discussed the nature of the drone threat, procurement processes, operational deployment, limitations of current systems, and future technological requirements for anti-drone operations.

Key Highlights:

- Punjab Police introduced the vehicle-mounted anti-drone system "Baazak" ("hawk eye" in Punjabi).
- Punjab Police became the first border state police force to directly engage drones crossing the international border.

- **The presentation covered:**
  - Drone threats along the Punjab border.
  - Deployment and implementation of anti-drone systems.
  - Operational experiences and challenges.
- **Punjab border regions experience:**
  - Approximately 80–100 drone movements daily.
  - Up to 150 drones during foggy conditions.
  - Amritsar Rural District was identified as the major hotspot for drone activity.
- **Drone smuggling was linked to:**
  - Narco-smuggling networks.
  - Cross-border criminal activity.
  - Narco-terror-gangster nexus.
- **Commonly recovered drones included:**
  - DJI Mavic 3.
  - Air 3S.
  - Matrice drones.
  - Modified hexacopters.
- **Recovered contraband included:**
  - Heroin.
  - Firearms.
  - Illegal materials.
- **Punjab Police established:**
  - Standing Committee on Drones.
  - High-powered procurement committee.
- **Procurement involved:**
  - MHA approval.
  - ARDTC evaluation and clearance.
  - Selection of approved systems only.
- **Punjab Police selected the ECIL anti-drone system based on:**
  - Operational suitability.
  - Mobility.
  - Budget considerations.
  - Soft kill capability.

- **Vehicle-mounted systems included:**
  - Foldable antennas.
  - Hydraulic lifting systems.
  - Silent generators.
  - Air fence operator interface.
- **Detection and jamming capabilities:**
  - Detection range: 5–8 km.
  - Detections achieved up to 38 km under favourable conditions.
  - Jamming range: approximately 2 km.
- **Key operational limitations included:**
  - Autonomous drones.
  - Detection versus jamming range gap.
  - RF detection and jamming conflicts.
- **Future requirements identified:**
  - Multi-sensor fusion.
  - AI-based drone classification.
  - Extended jamming range.

Key Outcomes:

- Deployment of the first vehicle-mounted portable anti-drone systems by a border state police force.
- Establishment of coordinated anti-drone operations between Punjab Police, BSF, and Army.
- Development of operational SOPs for anti-drone deployment and coordination.
- Identification of major drone smuggling patterns and operational timings.
- Enhanced detection of cross-border drone activity in Punjab border regions.
- Recovery and forensic analysis of drones used for smuggling heroin and firearms.
- Recognition of operational limitations in RF-based anti-drone systems.
- Planning for second-phase anti-drone capabilities including:
  - Cyber takeover systems.
  - AI-assisted classification.
  - Multi-sensor detection systems.
- Procurement and deployment of nine ECIL anti-drone systems within Punjab Police.
- Strengthening of investigative and forensic understanding related to drone-based crimes.

2. 5. 4 Tech Initiatives in Kerala (Online)

Presenter's Details:
Shri Ankit Ashokan IPS,
SP Kerala

Executive Summary:

The Kerala Police has undertaken a comprehensive digital transformation to enhance policing efficiency, cybersecurity, and citizen engagement. The approach combines **AI/ML-driven tools, centralized monitoring systems, and field-level technological empowerment** to shift from traditional policing to a **technology-enabled, intelligence-led model.**

Key initiatives include the establishment of a **Security Operations Center (SOC)** for real-time monitoring, deployment of **anti-drone systems (Eagle Eye)** for public safety, and creation of citizen-centric platforms like **Cyber Wall**. The focus is not only on advanced infrastructure but also on equipping field officers with **lightweight, practical tools** that improve investigation and operational efficiency.

The transformation emphasizes:

- Real-time data monitoring and cybersecurity.
- AI-powered investigation and analytics.
- Citizen-friendly digital interfaces.
- Predictive and data-driven policing.

Key Highlights:

1. Security Operations Center (SOC):

- Centralized monitoring of ~3,500 police systems.
- 24/7 surveillance for threats, vulnerabilities, and data breaches.
- Incident Response Teams for on-ground action.

2. Anti-Drone System – Eagle Eye:

- In-house developed system for VIP security and large events.
- Detects drones within a 5 km radius.
- Equipped with anti-drone guns for neutralization. AI-Powered Investigation Tools.

3. "Trace an Object" tool for crowd-sourced intelligence:

- Smart Object Finder for CCTV analysis using YOLO model.
- Facial Recognition System (FRS) integrated with policing apps.

4. Cyber Wall (Citizen Engagement Platform):

- WhatsApp-based AI system for fraud detection.
- Generates trust scores for suspicious links, emails, and numbers.
- Uses ML trained on real-time fraud databases.

5. Field-Level Enablement:

- Lightweight tools running on standard laptops.
- Offline Malayalam-English transliteration tool.
- Focus on usability without heavy infrastructure.

6. Data & AI Integration:

- Work on predictive policing and crime analytics.
- Development of LLM-based assistants for police and citizens.
- OCR and multilingual voice interfaces under development.

7. Collaboration & Innovation:

- Partnerships with universities and hackathons.
- Use of open-source tools for image enhancement and analysis.
- Continuous innovation through in-house development.

Key Outcomes / Takeaways:

1. Shift to Intelligence-Led Policing:

- Transition from reactive policing to predictive, data-driven operations.

2. Enhanced Cybersecurity & Monitoring:

- Real-time threat detection and faster incident response through SOC.

3. Improved Citizen Engagement:

- Easy reporting via WhatsApp-based Cyber Wall.
- Increased awareness and accessibility.

4. Operational Efficiency at Ground Level:

- Reduced manual workload with AI tools (CCTV analysis, translation, FRS).
- Faster investigation and documentation.

5. Advanced Surveillance & Public Safety:

- Anti-drone systems enhance security during critical events.

6. Data Integration & Accuracy:

- Reduced duplication in criminal records via facial recognition.
- Better profiling and identification.

7. Innovation-Driven Ecosystem:

- Continuous development through hackathons and collaborations.
- Adoption of open-source and AI technologies.

8. Successful Case Impact:

- AI-assisted investigation helped solve a 20-year-old triple murder case.

approx 200 No. of participants attended online.

2. 6 Mule Accounts Identification & Cybercrime Investigation

Presenter's Details:
Mr. Shahnaz Illyas, IPS,
Superintendent of Police, Cyber Crime, Tamil Nadu

Executive Summary:

This session focused on the growing threat of mule accounts and financial cybercrime, highlighting how fraudsters rapidly move money across multiple accounts, making tracing difficult. It emphasized key challenges such as fake identities, illegal apps, and conversion of funds into cryptocurrency. A data-driven approach using platforms like NCRP, cyber patrolling, and AI-based analysis was presented as essential for detecting patterns and identifying suspects. The session also covered proactive strategies like early detection of mule and victim accounts, monitoring fake ads and malicious websites, and tackling SIM box fraud using technical analysis. It highlighted that timely action, continuous monitoring, and strong data analysis are crucial for effective cybercrime investigation and prevention.

Key Highlights:

Data-Driven Investigation Systems:

- Integrates banking, telecom, and online data.
- Detects suspicious transaction patterns.
- Helps trace layered money transfers.

Mule Account Detection System:

- Identifies fake accounts.
- Flags high-frequency and burst transactions.
- Detects suspicious keywords (investment, profit, etc.).

Victim Identification & Alert System:

- Detects potential victims before complaint.
- Flags unusual withdrawals and transfers.
- Sends early warnings to prevent losses.
- Enables proactive policing.

Cyber Patrolling AI:

- Monitors KYC frauds, e-challan scams, APK malware.
- Detects fake websites and phishing links.
- Tracks fake ads on platforms (e.g., Meta).
- Prevents misinformation spread.
- Tracks suspicious sources (GitHub, fake websites).
- Detects emerging cyber threats early.

AI-Based Suspect Profiling:

- Identifies geographical hotspots of fraud.
- Profiles cybercriminal behavior.
- Supports targeted investigation.

Cryptocurrency Tracking Tools:

- Tracks conversion of stolen money into crypto.
- Follows digital financial trails.
- Helps in complex financial tracing.
- Supports recovery efforts.

SIM Box Detection System:

- Identifies illegal call routing setups.
- Detects international fraud masked as local calls.

Telecom Analysis Tools (TDR, IMEI, IPDR, SIP Analysis):

- Tracks communication patterns.
- Identifies suspicious devices and IPs.
- Detects network-level fraud operations.
- Locates suspicious IP addresses.
- Maps illegal communication networks.

2. 7 POLNET & Public Protection Communication Systems

Presenter's Details:
Shri Ashim Sen, IPS,
Joint Director, DCPW

Executive Summary:

The session focused on secure communication systems like POLNET that ensure reliable connectivity for police forces, especially during disasters and critical operations. POLNET, a satellite-based network using GSAT-17, enables voice, video, and data communication even in remote areas through VSAT terminals. While it provides strong operational support, challenges like network congestion and the need for secure digital encryption were also highlighted. The session introduced BB-PPDR as a next-generation system offering encrypted, low-latency, and nationwide seamless communication. Overall, it emphasized that robust communication infrastructure is essential for effective coordination, quick response, and disaster management in policing.

Key Highlights:

POLNET (Police Telecommunication Network)	• Provides satellite-based secure communication • Works in remote and disaster-affected areas • Supports voice, video calls, and conferencing • Ensures uninterrupted police connectivity
GSAT-17 (Satellite Backbone)	• Enables nationwide communication coverage • Supports reliable data transmission • Ensures connectivity independent of ground networks
POLNET Hub (Central Control System)	• Manages entire communication network • Controls data flow and connectivity • Ensures coordinated communication across units
VSAT	• Provides on-ground satellite communication access • Available as static and portable units • Enables field-level connectivity in remote locations
Portable VSAT Systems	• Quick deployment (30–45 minutes) • Useful during disasters and emergency operations • Ensures rapid communication setup in field conditions
Encrypted Digital Communication (AES-based)	• Secures sensitive police communication • Prevents interception and data leaks • Ensures safe transmission of operational information
BB-PPDR (Broadband Public Protection & Disaster Relief Network)	• Next-generation secure communication system • Provides low-latency, real-time connectivity • Supports body cameras and modern devices • Enables seamless nationwide coordination

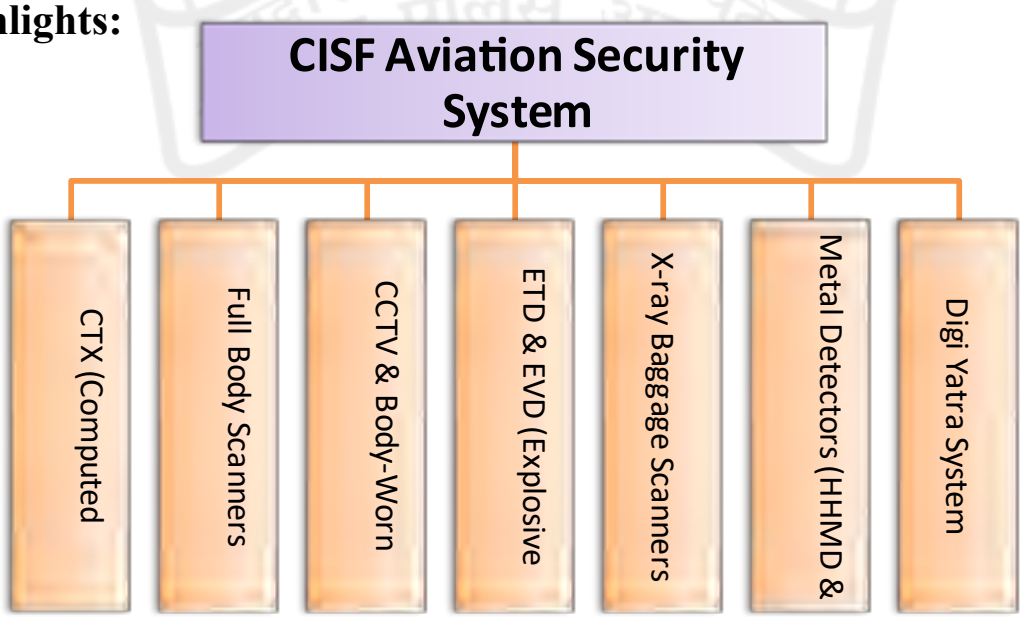
2. 8 Aviation Security and Emerging Threats

Presenter's Details:
Senthil Avoodai Krishna Raj S, IPS,
DIG, CISF

Executive Summary:

This session focused on aviation security in India, covering existing systems, emerging threats, and future technologies. It explained the current security structure across airports, with Central Industrial Security Force and state police units sharing responsibilities. The session highlighted modern security tools such as access control systems, screening technologies, and real-time surveillance for effective monitoring. It also discussed recent challenges like GPS spoofing, airline disruptions, and evolving technical threats. Future solutions including full-body scanners, CTX systems, and anti-drone technologies were emphasized. Overall, the session showed that aviation security is becoming increasingly technology-driven to handle complex and dynamic threats.

Key Highlights:



CISF Aviation Security System:

- Secures major airports across India.
- Handles anti-hijacking, protection, and surveillance.
- Ensures coordinated airport security operations.

Digi Yatra System:

- Enables seamless passenger processing.
- Uses facial recognition for entry/boarding.
- Reduces congestion and improves efficiency.

Metal Detectors (HHMD & DFMD):

- Detects metallic threats on passengers.
- Ensures primary level security screening.
- Prevents weapon entry.

X-ray Baggage Scanners:

- Screens luggage for prohibited items.
- Detects hidden threats.
- Supports security checks efficiently.

ETD & EVD (Explosive Detection Systems):

- Detects explosive substances.
- Enhances threat identification accuracy.

CCTV & Body-Worn Cameras:

- Enables real-time surveillance.
- Assists in evidence collection.
- Improves accountability and monitoring.

Full Body Scanners (Advanced Screening):

- Detects metallic and non-metallic threats.
- Improves passenger screening accuracy.
- Enhances overall security levels.

CTX (Computed Tomography X-ray Systems):

- Provides detailed 3D baggage scanning.
- Improves explosive detection capability.
- Reduces false alarms.

2. 9 IT Initiatives by SVPNPA/ Cyber X

Presenter's Details:
Shri Paramesh,
Cyber X

Executive Summary:

The session briefly showcased the IT initiatives of the academy through the Cyber X lab established in the MTC building. Cyber X, previously known as NDCRTC, was established in 2015 in NPA with technical support from CDAC Hyderabad as a premier centre of excellence for cybercrime investigation and digital forensics. The primary mandate of the unit is capacity building and training of police officers across India through onsite and outreach programmes.

The presentation covered the domains handled by CyberX, the training activities conducted for police agencies, and demonstrations of solutions developed by the CyberX team, including Facial Recognition Systems (FRS), dark web intelligence platforms, deep web monitoring, and related investigative technologies. Demonstrations highlighted the operational use of face recognition systems for photo retrieval, suspect identification, and investigative lead generation using data indexing, facial feature extraction, and data leak repositories.

Key Highlights:

- 1. CyberX lab is located in the MTC building and functions as a premier centre of excellence established in 2015 in NPA with technical support from CDAC Hyderabad.

2. The primary mandate of CyberX is training police officers across India in:

- Cybercrime investigation.
- Digital payment frauds.
- Open source intelligence.
- Digital crime scene management.
- Cyber security.
- Malware and network analysis.
- Mobile forensics.
- Digital forensics.
- IPDR and VOIP.
- Blockchain.
- Cryptocurrency.
- Dark web related investigation.

3. CyberX has trained more than 19,698 officers through online, offline, hybrid, and outreach training programmes.

4. Solutions developed by the CyberX team include:

- Dark web intelligence.
- Deep web monitoring.
- Facial Recognition System (FRS).
- SOC dashboard.

5. The FRS platform was developed to allow course participants to retrieve photographs taken during training programmes.

6. The FRS system works by:

- Uploading a photograph.
- Detecting faces from the uploaded image.
- Extracting facial features.
- Generating a unique facial fingerprint.
- Searching indexed databases for matching photographs.

7. The facial recognition process uses 106 facial data points including:

- Eyebrow dimensions.
- Distance between eyebrows.
- Nose length.
- Nose width.

8. The system supports:

- Match percentage thresholds.
- Result filtering.
- Exporting photographs into ZIP files.
- Course-wise and date-wise categorization.

9. The system demonstrated successful recognition even in:

- Side profile images.
- Slightly blurred images.
- Partial face visibility.

10. Another platform named "Face One" was demonstrated with wider datasets for investigative use.

11. A Delhi Jain temple gold theft case was demonstrated where:

- CCTV footage captured the suspect.
- Facial recognition identified a matching profile image.
- A mobile number linked to a Paytm account was identified.
- Location-based services were used.
- The suspect was arrested within 24 hours.

12. The system uses indexed data collected from multiple platforms including:

- WhatsApp.
- Paytm.
- PhonePe.
- Viber.
- Truecaller.
- Facebook.
- Twitter.
- Instagram.
- TikTok.

13. A dark web solution was also discussed where leaked internet and dark web data are downloaded, indexed, and searched for investigative leads.

Key Outcomes:

- Establishment of CyberX as a centre for cybercrime and digital forensics training.
- Training of more than 19,698 police officers across India.
- Development of facial recognition systems for:
  - Photograph retrieval.
  - Person identification.
  - Investigative support.
- Creation of searchable indexed repositories for leaked internet and dark web data.
- Generation of investigative leads through facial recognition and linked mobile number identification.
- Successful support in criminal investigations including:
  - Delhi Jain temple gold theft case.
  - Airport bomb threat investigations.
  - Delhi blast related investigations.
- Enhanced capability for digital investigation through:
  - Data indexing.
  - Facial feature extraction.
  - Social media and application data correlation.
  - Dark web intelligence analysis.

2. 10 Problem-Driven Innovation in Policing: Goa Model

Presenter's Details:
Shri Rahul Gupta, IPS

Executive Summary:

The session "Problem-Driven Innovation in Policing: Goa Model" outlines a structured, problem-first approach to modernizing Goa policing through technology, AI, and institutional innovation. It identifies key challenges—citizen interface delays, manpower constraints, reactive policing, and inefficient enforcement—and addresses them through targeted, scalable solutions.

The model emphasizes building a sustainable innovation ecosystem via academic partnerships, hackathons, and in-house AI capabilities, enabling rapid development and deployment of tools such as cloud-based helplines, AI investigation assistants, and cyber detection systems.

By integrating AI-driven tools for fraud detection, intelligence generation, and proactive monitoring, the Goa Police transitions from reactive to intelligence-led policing, improving response times, operational efficiency, and citizen experience. The approach is iterative, collaborative, and outcome-focused, demonstrating measurable impact in fraud reduction, reporting efficiency, and workload optimization.

Key Highlights:

1. Problem-First Policing Approach:

- Focus on real operational bottlenecks:
  - Citizen interface delays.
  - Limited manpower vs increasing workload.
  - Reactive policing.
  - Inefficient enforcement processes.

2. Innovation Ecosystem (Goa Model):

- Academic MoUs (BITS Pilani, IIT Goa, NIT Goa).
- Hackathon-driven solution development.
- AI-ML Lab for in-house capability building.
- Collaboration over traditional procurement.

3. Citizen Interface Transformation:

- 1930 cloud-based helpline for instant complaint capture.
- AI-based co-pilot and visitor assistance tools.
- Goa Police App for tenant verification and upcoming services.

4. Workload Reduction & Productivity:

- AI-based investigation assistance.
- Deep Trace for intelligence aggregation - provides initial intelligence generation about the target including possible names, mobile numbers, addresses, PAN, DIN, and vehicle details — all in one place for investigating officers.
- e-Beatbook and Night Vigil apps for field operations - Testing Phase.

5. Shift to Proactive Policing:

- AI tools like SpotTheScam and Radical Content Analyser.
- Cyber patrolling tools and PRISM intelligence unit.
- Early detection of fraud and radicalisation patterns.

Fig: SpotTheScam Web Page

6. Traffic & Enforcement Optimization:

- QuickPass system to reduce redundant checks.
- Improved commuter experience and transparency.

Fig: Vehicle Check details

7. Measurable Impact:

- 30% reduction in fraud amount.
- Increased complaint registration and structured data capture.
- Significant operational efficiency gains.

8. Measurable Impact:

- 30% reduction in fraud amount.
- Increased complaint registration and structured data capture.
- Significant operational efficiency gains.

Key Outcomes / Takeaways:

1. Transition to Intelligence-Led Policing:

- Movement from reactive response to predictive and preventive policing.

2. Enhanced Citizen Experience:

- Faster response, reduced friction, and improved service delivery.

3. Improved Operational Efficiency:

- Automation reduces manual workload and cognitive burden on officers.

4. Data-Driven Decision Making:

- AI tools enable faster pattern recognition and actionable insights.

5. Scalable Innovation Model:

- "Build → Test → Deploy → Iterate" ensures rapid and adaptable implementation.

6. Strong Collaboration Framework:

- Partnerships with academia and startups enable continuous innovation.

7. Tangible Impact on Crime Handling:

- Faster fraud response, reduced escalation, and improved reporting rates.

2. 11 Challenges in Technology Implementation in Policing & Its Experiences

Presenter's Details:
Shri Senthil Avoodai Krishna Raj S, IPS,
DIG CISF

Executive Summary:

The presentation "Challenges in Technology Implementation in Policing & its Experiences" examines the organizational, technical, and operational barriers in adopting digital systems in policing, supported by field experience and empirical analysis. It highlights initiatives in Uttarakhand Police while identifying key constraints such as institutional inertia, limited digital literacy, budget limitations, fragmented systems, and multi-stakeholder complexity.

It emphasizes that technology adoption is not purely technical but depends significantly on human factors, training, and organizational culture, supported by global insights showing low conversion of innovations into operational use.

Using the TAM 2 model and a survey of 1500+ personnel, the study evaluates adoption drivers such as usefulness, ease of use, and training, revealing demographic and experiential differences that require targeted interventions.

The presentation concludes with a strategic framework based on the "4 A's" (Affordable, Accessible, Adaptable, Amalgamable) and a balanced top-down and bottom-up approach for scalable and sustainable implementation.

Key Highlights:

1. Existing Technological Initiatives:

- Multiple systems implemented:
  - E-FIR, E-Malkhana, E-Beat, IO Mobile App.
  - CCTNS integrations, NAFIS, MedLeaPR.
  - Police mobile applications and monitoring systems.

2. Core Implementation Challenges:

- Organizational inertia and resistance to change.
- Low digital familiarity and training gaps.
- Budgetary and infrastructure constraints.
- Geographical and operational challenges.
- Multi-stakeholder coordination (ICJS ecosystem).

3. Technical & Systemic Issues:

- Fragmented and dispersed databases.

- Rapid evolution of cyber technologies.
- Limited indigenous technology development.
- Concerns around data security and resilience.
- Lack of specialized technical cadre.

4. Human-Centric Barriers:

- Age, education, and experience influence adoption.
- Variation across ranks and districts.
- Dependence on training and usability of systems.

5. Empirical Study (TAM 2 Model):

- Survey of 1500+ personnel.
- Key parameters: usefulness, ease of use, training, social influence.
- Strong reliability (Cronbach Alpha > 0.7).
- Highlights behavioral aspects of technology adoption.

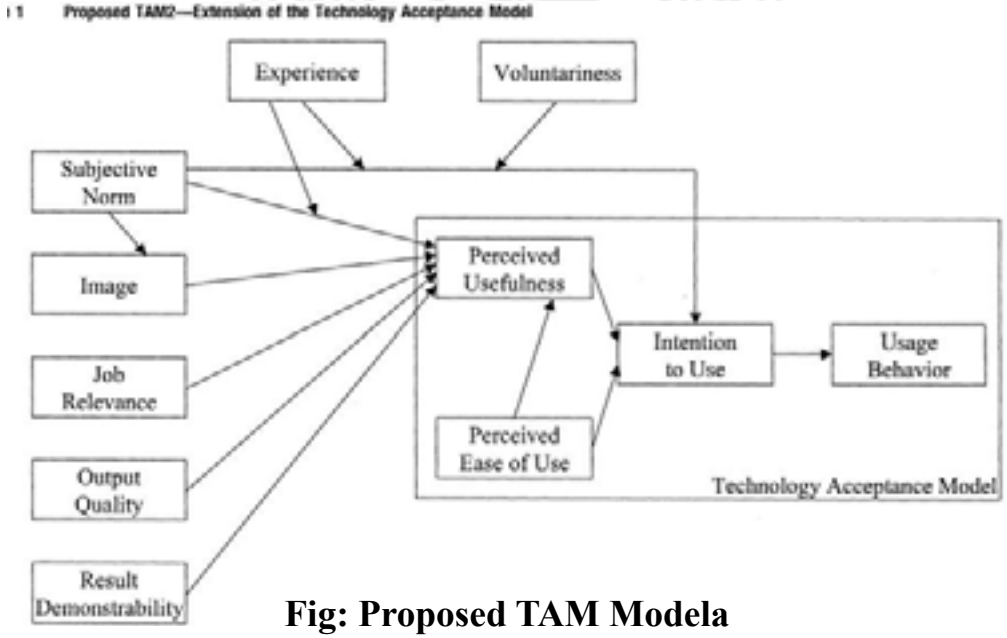


Fig: Proposed TAM Modela

6. Key Behavioral Insights:

- Younger personnel are early adopters (“champions”).
- Senior personnel show slower adoption (“laggards”).
- Higher ranks show stronger commitment.
- Experience increases satisfaction and perceived usefulness.
- Gender impact largely neutral.

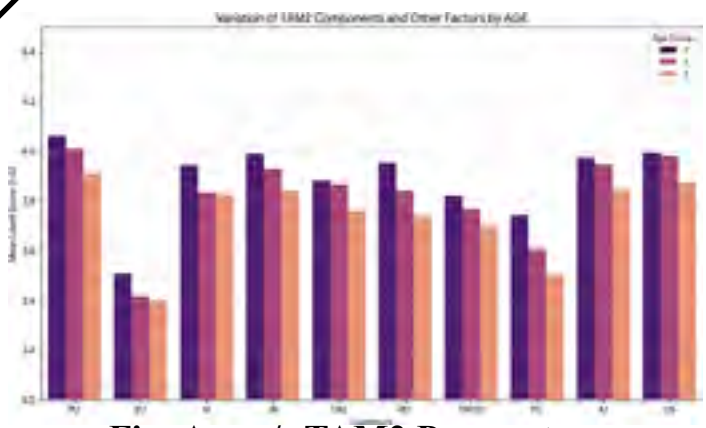


Fig: Age v/s TAM2 Parameters

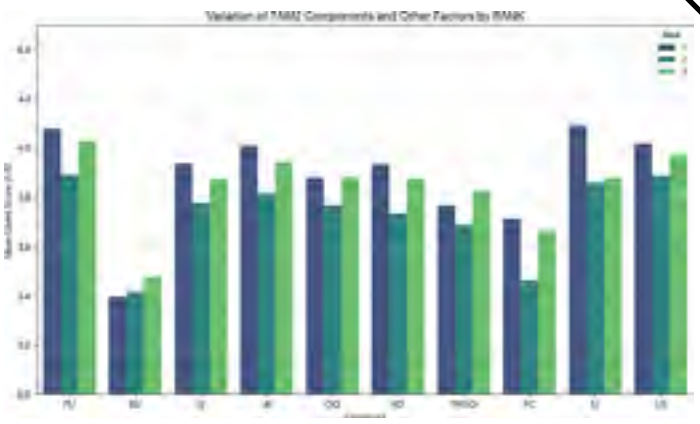


Fig: Rank v/s TAM2 Parameters

7. Global Insight:

- Low success rate in scaling innovations (example: Netherlands police ~5%).
- Highlights gap between development and real-world deployment.

Key Outcomes:

1. Technology Adoption is Human-Driven:

- Success depends more on people, training, and mindset than tools.

2. Need for Structured Implementation Strategy:

- Combine top-down policy direction with bottom-up adoption.

3. Importance of Capacity Building:

- Continuous training and creation of "tech champions" is critical.

4. Standardization & Integration Required:

- Reduce fragmentation across systems and databases.

5. Data Security & Resilience Priority:

- Systems must be robust against failures and cyber threats.

6. Scalable Framework for Adoption:

- "4 A's" (Affordable, Accessible, Adaptable, Amalgamable) as guiding principles.

7. Evidence-Based Policymaking:

- Use models like TAM 2 and field surveys to guide implementation decisions.

2. 12 Cyber Auditor

Presenter's Details:
Rajesh Kumar Pal, C.E.O.
Mobisec Technologies

Executive Summary:

Cyber Auditor is a specialized cyber security auditing solution designed to strengthen the integrity, security, and reliability of digital systems used in policing. In the context of modern investigations, where digital evidence plays a critical role, the tool ensures that systems remain secure, compliant, and resistant to cyber threats.

It supports law enforcement agencies by identifying vulnerabilities, ensuring proper configurations, and safeguarding sensitive investigative data. The tool is particularly relevant in environments where **data confidentiality and evidence integrity must be preserved,** especially prior to charge sheet filing.

Cyber Auditor contributes to a secure digital ecosystem by enabling proactive risk detection, enhancing system resilience, and supporting forensic readiness in cybercrime investigations.

Key Highlights:

1. Cyber Security Auditing Capability:

- Performs comprehensive system and network audits.
- Identifies vulnerabilities and security gaps.
- Ensures compliance with cyber security policies and standards.

2. Investigation-Centric Security:

- Designed for handling sensitive investigation data.
- Supports secure environments (restricted / controlled systems).
- Ensures integrity of digital evidence before legal proceedings.

3. Cross-Platform Compatibility:

- Supports multiple operating systems:
  - Linux.
  - Windows.
  - macOS.
  - Chromebooks.
- Enables flexibility across different policing infrastructures.

4. Threat Detection & Risk Identification:

- Detects:
  - Weak configurations.
  - Unauthorized access points.
  - Potential malware threats.
- Helps in early identification of system risks.

5. Support for Digital Forensics:

- Enhances forensic readiness of systems.
- Ensures proper handling and preservation of digital evidence.
- Assists investigators in maintaining legally admissible data.

6. Integration with Policing Ecosystem:

- Complements systems like:
  - Security Operations Center (SOC).
  - Cyber intelligence platforms.
- Acts as a preventive security layer in digital policing.

7. Secure Investigation Environment:

- Helps maintain:
  - Data confidentiality.
  - System integrity.
  - Controlled access to sensitive information.

Key Outcomes:

1. Strengthened Cyber Security:

- Improved protection of police IT infrastructure.
- Reduced risk of cyber attacks and data breaches.

2. Enhanced Investigation Integrity:

- Secure handling of digital evidence.
- Reduced chances of data tampering or leakage.

3. Improved Operational Reliability:

- Systems remain stable, secure, and audit-compliant.
- Increased trust in digital policing tools.

4. Reduced Risk Exposure:

- Early detection of vulnerabilities minimizes threats.
- Preventive approach to cyber security.

5. Support to Investigation Officers:

- Provides a secure environment for conducting investigations.
- Reduces technical risks during evidence collection and analysis.

6. Better Compliance & Governance:

- Ensures adherence to legal and cyber security standards.
- Supports structured and accountable digital processes.

7. Foundation for Secure Digital Policing:

- Acts as a critical component in modern, technology-driven policing.
- Strengthens overall cyber resilience of law enforcement agencies.

2. 13 Presentation on CCTNS & ICJS

Presenter's Details:
Shri Jayant Singh, IPS,
AD,NCRB.

Executive Summary:

The National Crime Records Bureau (NCRB) is spearheading the digital transformation of India's policing and criminal justice ecosystem under the vision of "One Country, One Data, Once Entry."

Through the implementation of systems such as CCTNS (Crime and Criminal Tracking Network and Systems) and ICJS (Interoperable Criminal Justice System), NCRB has enabled seamless data integration across police, courts, prisons, prosecution, and forensic departments.

The transformation focuses on:

- Digitization of criminal justice processes
- Real-time data sharing and analytics
- Integration across multiple agencies
- Enhanced transparency and citizen services

Advanced technologies such as AI/ML and Natural Language Processing (NLP) are being leveraged to improve investigation efficiency, predictive policing, and decision- making.

Key Highlights:

1. NCRB Mandate and Role:

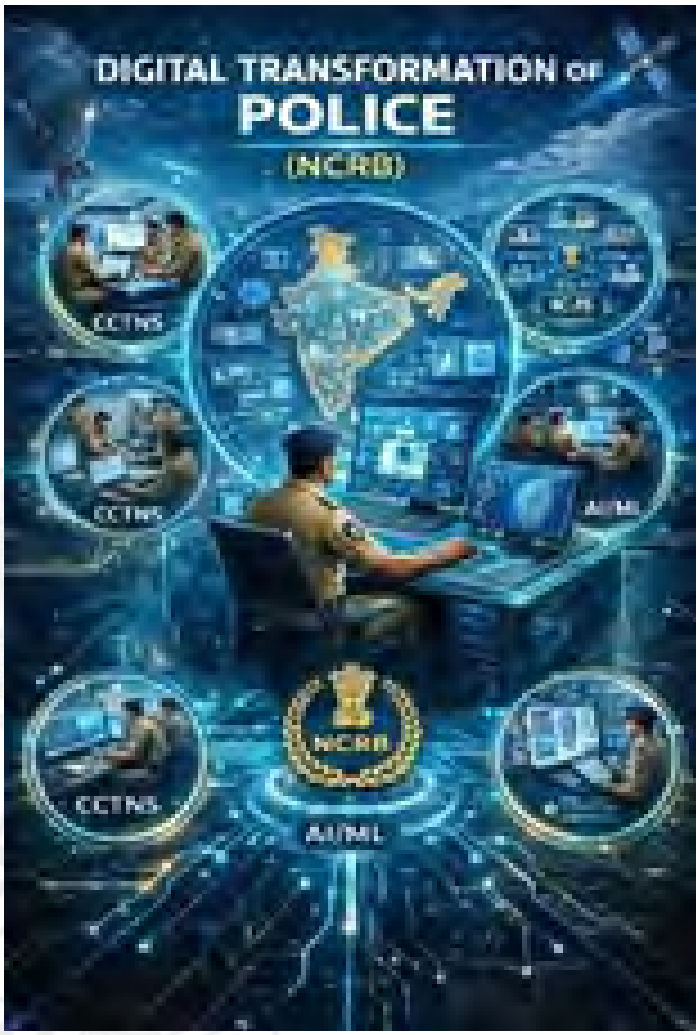
- National repository for crime and criminal data.
- Supports investigation and inter-agency coordination.
- Monitors and implements CCTNS and ICJS projects.
- Develops national-level IT systems and databases.

2. CCTNS (Crime and Criminal Tracking Network and Systems):

Specifications / Features:

- 100% coverage of police stations (17,798).
- Nationwide crime and criminal database (~42 crore records).
- Real-time FIR registration and updates.
- Citizen portals implemented across all States/UTs.
- National-level search and data synchronization.

3. ICJS (Interoperable Criminal Justice System).:



Specifications / Features:

- Integration of:
  - Police.
  - Courts.
  - Prisons.
  - Prosecution.
  - Forensics.
- Secure and seamless data exchange.
- Integration with other government databases.
- Supports analytics for decision-making.

4. Supporting Digital Systems:

- e-Prisons, e-Prosecution, e-Forensics.
- e-Sakshya (digital evidence management).
- e-Summons (digital court process delivery).
- Nyaya Shruti (virtual court system).
- MedLeaPR (medical reporting platform).
- NAFIS (fingerprint identification system).
- CrPI System (biometric identification database).

5. AI/ML Integration:

- AI-based FIR analysis and section prediction.
- Identification of crime patterns (modus operandi).
- Predictive policing using historical and geospatial data.
- Crime network analysis.
- AI-based citizen chatbot services.

6. CCTNS 2.0 (Next-Generation System):

Key Enhancements:

- Integration of AI/ML and analytics.
- Improved UI/UX and ease of use.

- Mobile-enabled policing.
- Enhanced citizen services.
- Centralized cloud hosting (MeghRaj 2.0).
- Integration with ICJS and other systems.
- Real-time data exchange.

Status:

- Development in advanced stage.
- Pilot rollout initiated.
- Migration planned in phased manner.

Key Outcomes / Takeaways:

1. End-to-End Digital Transformation:
   - Complete digitization of the criminal case lifecycle from FIR to prosecution.
2. Real-Time Monitoring & Tracking:
   - Continuous tracking of FIRs and investigation progress across all levels.
3. Enhanced Inter-Agency Coordination:
   - Seamless information sharing between multiple law enforcement agencies.
4. Elimination of Redundancy:
   - Removal of duplicate data entry through integrated and unified systems.
5. Strengthened Accountability & Governance:
   - Improved monitoring mechanisms ensuring transparency and responsibility.
6. Citizen-Centric Transparency:
   - Increased public trust through accessible and transparent policing services.
7. National Crime Data Integration:
   - Creation of a centralized nationwide crime and criminal database.
8. Data-Driven & Predictive Policing:
   - Use of analytics and AI for proactive decision-making and crime prevention.
9. Improved Investigation & Prosecution Efficiency:
   - Faster case handling and better coordination leading to improved outcomes.

Approximately 200 No. of participants attended online.

PART - III

Tech Exhibition

Tech Exhibition

The Tech Exhibition, which provided participants an opportunity to see, understand, and interact with various technology-based tools, products, applications, and equipment relevant to policing, investigation, internal security, and field operations. The exhibition served as a practical learning platform where selected organisations and technology partners associated with police, DRDO, NFSU, and other law enforcement-related institutions showcased innovative solutions designed to strengthen policing capabilities. Care was taken to include firms and agencies having direct relevance or working association with police and security organisations, rather than purely commercial vendors. The exhibition was also witnessed by around 160 plus IPS probationers, thereby extending its learning value to young officers who will be leading field units in the future.

The exhibition complemented the classroom sessions by giving officers direct exposure to operational technologies that can be used for crime detection, cyber forensics, surveillance, communication, counter-drone operations, traffic management, citizen services, and field-level policing. It included displays by Telangana Police, CDAC Trivandrum, NFSU Goa, the Cyber X team of SVP NPA, DRDO and its industry partners, NTRO, and other selected technology developers. A wide range of products and systems were presented, including police applications, traffic management tools, cyber forensic applications, facial recognition and digital investigation tools, bulletproof jackets and helmets, small arms, ambulance bike technology, handheld and portable anti-drone systems, drones with weapon-mounted capability, ground penetrating radar for IED detection, and lightweight explosive identification systems.

Special importance was given to DRDO-developed and security-oriented products, including anti-drone systems, handheld ground penetrating radar, portable RF counter-drone systems, mobile forensic suites, secure communication equipment, and surveillance solutions. The exhibition also highlighted practical policing platforms such as CCTNS 2.0, TSCOP, e-Petty Case Application, Integrated Patrol Management System, IMCAP, Hawk Eye Ultra, Citizen Portal, and other digital tools aimed at improving investigation, patrol management, citizen engagement, and real-time decision-making. Overall, the Tech Exhibition enriched the workshop by transforming theoretical discussions into practical demonstrations and enabling officers and probationers to assess how emerging technologies can be adopted, customized, and deployed to meet real policing challenges. It reinforced the workshop's central message that technology, when aligned with field requirements, can become a powerful force multiplier for modern policing.


9X19MM SMG (ASMI)
9X19MM SMG (ASMI)









Details of Tech Exhibition Products, Apps and Tools		
S.No	**Description of Product/tools/Apps**	**Organisation**
1.	Apps developed by Telangana Police	T.G. Police
2.	Traffic Management	T.G. Police
3.	App on Cyber Forensics	CDAC, Trivandrum
4.	Three apps (startups)	NFSU, Goa
5.	Cyber X team	SVP NPA
DRDO Developed Products		
6.	DRDO developed product – Bullet proof jacket and helmet	RVB Shorluble Industry Pvt Ltd, Kanpur
7.	Ugram Assault Rifle, ULMG	Dvipa Industries, Hyderabad.
8.	Display of ASMI pistol (9X19mm) and & Light Machine Gun	Lokesh Machines, Hyderabad.
9.	3D Presentation of RAKSHITA – Ambulance bike	INMAS and Skyline Power Solutions, New Delhi
10	Hand held & Portable Anti Drone systems for VVIP & Vital installation protection	DLRL, DRDO, Hyderabad.
11	The team will represent Cyronics Innovation Labs	NTRO, Pune
12.	Drone with Gun (Short & Long range)	DRDO, Hyderabad.
13.	Hand held Ground Penetration Radar for IED detection	Astra Microwave, Hyderabad.
14.	Light weight Explosive Identification System	Urmi Systems, Hyderabad.
15.	Small arms presentation	ARDE (DRDO), Pune

Handheld Ground Penetrating Radar (HHGPR)

Features:

- Operates in the 1.5–3 GHz frequency range with subsurface penetration up to ~20 meters and ~5 cm resolution.
- Equipped with Android-based touchscreen interface supporting real-time 2D and 3D visualization.
- Lightweight (< 4 kg) handheld system designed for portable and rapid deployment.

Outcomes:

- Enables accurate detection of subsurface objects such as landmines, IEDs, buried utilities, and voids.
- Enhances operational safety by reducing the need for manual probing in hazardous environments.
- Provides real-time visualization, improving decision-making for field operators.
- Ensures high precision and faster detection, increasing mission efficiency.
- Supports multi-domain applications, including defence operations, disaster response, and civil engineering.
- Overcomes limitations of traditional survey methods such as bulkiness and slower data acquisition.
- Improves infrastructure assessment and geological analysis in varied terrains.

Presenter's Details:

Astra Microwave Products Ltd., Hyderabad
Contact: +914046618000, mktg@astramwp.com
www.astramwp.com

Handheld Ground Penetrating Radar (HHGPR)

QUASAR Portable Lightweight ESM System

Features:

- Frequency coverage: 30 MHz – 6 GHz (extendable to 18 GHz) with modular multi-band support.
- Integrated COMINT & ELINT decoding suite (GSM, IMSI catcher, SATCOM, drones).
- High sensitivity (–117 dBm) with burst signal detection & de-hopping capability.

Fig-QUASAR Portable Lightweight ESM System

Outcomes:

- Enables real-time interception and monitoring of diverse RF signals.
- Strengthens electronic and communication intelligence capabilities.
- Ensures reliable performance in harsh terrains and adverse weather conditions.
- Provides portable and rapid deployment for field operations.
- Enhances operational flexibility (static and vehicle-mounted deployment).
- Facilitates advanced signal analysis and visualization (e.g., 3D waterfall display).
- Supports multi-threat monitoring, including drones and digital communication systems.

Fig-multi-band Antenna Array

Presenter's Details:

Cyronics Innovation Labs Pvt. Ltd., Pune

QUASAR HF Manpack SDR

Features:

- Operates in 1.8 MHz – 30 MHz HF band with support for SSB and CW communication modes.
- Configurable transmit power (up to 100W) with high frequency stability (±0.1 ppm).
- Portable (<10 kg) with VSWR protection and USB-based configuration.

Outcomes:

- Provides reliable long-range communication in remote and rural areas.
- Enables connectivity in infrastructure-denied environments.
- Enhances operational flexibility through software-defined radio architecture.
- Improves mobility and rapid deployment for field personnel.

Ensures stable communication under adverse environmental conditions.

Supports mission-critical communication continuity during field operations.

Presenter's Details:

Cyronics Innovation Labs Pvt. Ltd., Pune.

FIG-QUASAR HF Manpack SDR

QUASAR UHF Manpack SATCOM Terminal

Features:

- Operates in the UHF band using Indian geostationary satellites with multiple modulation schemes.
- Provides secure communication (256-bit encryption) with ~19.2 kbps data rate.
- Lightweight (~7.5 kg) with up to 12 hours endurance and GIS-based features.

Outcomes:

- The system provides secure beyond-line-of-sight communication.
- It ensures reliable connectivity in remote and difficult terrains.
- It enhances situational awareness through GIS integration.
- It supports continuous communication in hostile environments.
- It improves command and control coordination during operations.

Presenter's Details:

Cyronics Innovation Labs Pvt. Ltd., Pune.

Fig-UHF Manpack SATCOM Terminal

CHITRAGUPT – AI-Powered Mobile Forensics Suite Features:

- AI-powered field-deployable mobile digital forensics system for on-site evidence identification, extraction, and analysis.
- High-performance architecture: Intel Core i7 (14th Gen), 32 GB DDR5 RAM, RTX 4070 GPU (~321 AI TOPS), NVMe Gen4 SSD.
- Supports AI-driven analytics, real-time data processing, and multi-device/multi-OS compatibility.
- Ensures secure, tamper-proof evidence handling with rapid, lab-independent forensic workflows.

Outcomes:

- Enables real-time, on-site digital forensic investigations.
- Reduces dependency on centralized forensic laboratories.
- Significantly improves speed and efficiency of investigations.
- Enhances accuracy through AI-driven analysis and insights.
- Ensures integrity and security of digital evidence.
- Supports faster decision-making and intelligence generation.
- Strengthens capabilities of law enforcement, defence, and investigative agencies.

Presenter's Details:

Forensic Cyber Tech Machines (FCTM)
7th floor, Shivarth The Ace, Besides Courtyard by Marriott,
Sindhu Bhavan Road, Ahmedabad - 380054
info@forensiccybertech.com
www.forensiccybertech.com, +919099556604

1. CCTNS 2.0 (Crime and Criminal Tracking Network & Systems 2.0)

Features:

- End-to-end, intelligence-led policing platform with standardized workflows from complaint registration to case closure.
- Supports role-based operations and real-time data sharing across police, courts, prisons, and forensic units.
- Provides mobile access, dashboards, digital evidence management, and "One Data – One Entry" architecture for consistency.

CCTNS

Outcomes:

- Improves quality of investigations and increases conviction rates.
- Enhances data accuracy, accountability, and transparency across the system.
- Enables seamless inter-agency coordination and information sharing.
- Strengthens technology-driven and citizen-centric policing practices.
- Reduces duplication of data entry and procedural delays.
- Facilitates faster decision-making through real-time insights and alerts.

2. TSCOP (Telangana State COP App)

Features:

- Mobile application for frontline officers with real-time access to crime and
- criminal databases.
- Enables on-field suspect/vehicle
- verification, GPS-based patrol tracking, and incident reporting.
- Provides access to CCTV networks, evidence sources, and crime scene documentation tools.

TSCOP (Telangana State COP App)

Outcomes:

- Improves field-level efficiency and faster decision-making for police personnel.
- Enables real-time verification of suspects and vehicles, enhancing response capability.
- Strengthens data accessibility for frontline policing operations.
- Enhances patrol monitoring and accountability through GPS-based tracking.
- Supports efficient incident reporting and documentation at the scene.
- Improves coordination with control rooms and investigative units.

3. e-Petty Case Application

Features:

- Mobile-based enforcement tool for on-the-spot registration and processing of petty offences.
- Captures offender details, photos, and digital evidence, with instant digital charge sheet generation.
- Integrates with court systems and offender databases for tracking repeat violations.

Outcomes:

- Enables faster disposal of minor offences, reducing backlog.
- Enhances transparency and accountability in enforcement processes.
- Helps identify and track repeat offenders, improving deterrence.
- Prevents escalation of petty crimes into serious offences.
- Improves efficiency of field officers through digital workflows.
- Strengthens integration between enforcement and judicial systems.

4. IPMS (Integrated Patrol Management System)

Features:

- GPS-enabled patrol monitoring system for real-time tracking of vehicles and personnel.
- Provides route monitoring, activity status tracking, and nearest unit identification for dispatch.
- Generates patrol analytics and performance reports for operational assessment.

Outcomes:

- Reduces response time to incidents through efficient unit allocation.
- Optimizes patrol deployment and resource utilization.
- Enhances visible policing and field supervision.
- Improves accountability and monitoring of patrol activities.
- Enables data-driven decision-making through patrol analytics.
- Strengthens coordination between control rooms and field units.

5. IMCAP (Intelligent Mapping of Crime and Accidents for Police)

Features:

- GIS-based platform for mapping crimes, accidents, CCTV locations, and patrol infrastructure.
- Provides visualization of hotspots, spatial patterns, and crime trends with analytical tools.
- Generates data-driven reports to support strategic planning and decision-making.

IMCAP (Intelligent Mapping of Crime and Accidents for Police)

Outcomes:

- Enables data-driven crime prevention and resource allocation strategies.
- Improves identification of crime hotspots and emerging trends.
- Strengthens proactive policing and strategic planning.
- Enhances situational awareness through geospatial visualization.
- Supports efficient deployment of patrol units based on hotspot analysis.
- Facilitates better coordination across police units using shared spatial data.

6. Hawk Eye Ultra

Specifications:

- Citizen-centric mobile application for reporting crimes, suspicious activities, and violations.
- Supports photo/video evidence submission, SOS, and women safety features.
- Provides real-time alerts, notifications, and access to missing persons and stolen vehicle data.

Hawk Eye Ultra

Outcomes:

- Strengthens citizen–police collaboration and trust.
- Enables faster reporting and response to incidents.
- Enhances community participation in policing efforts.
- Improves situational awareness through real-time alerts and updates.
- Supports women's safety with emergency SOS features.
- Facilitates crowdsourced intelligence for better law enforcement outcomes.

7. Citizen Portal

Specifications:

- Digital platform for citizen police services, including online complaint/petition filing and FIR status tracking.
- Provides verification services, document downloads, and access to public data (missing persons, stolen vehicles).
- Integrates e-Challan and other online services to enable end-to-end digital interaction.

Citizen Portal

Outcomes:

- Improves transparency and accessibility of police services.
- Reduces dependency on physical visits to police stations.
- Enhances citizen convenience and ease of service delivery.
- Promotes digital governance and efficient public service systems.
- Speeds up service delivery and grievance redressal processes.
- Strengthens public trust through accessible and user-friendly platforms.

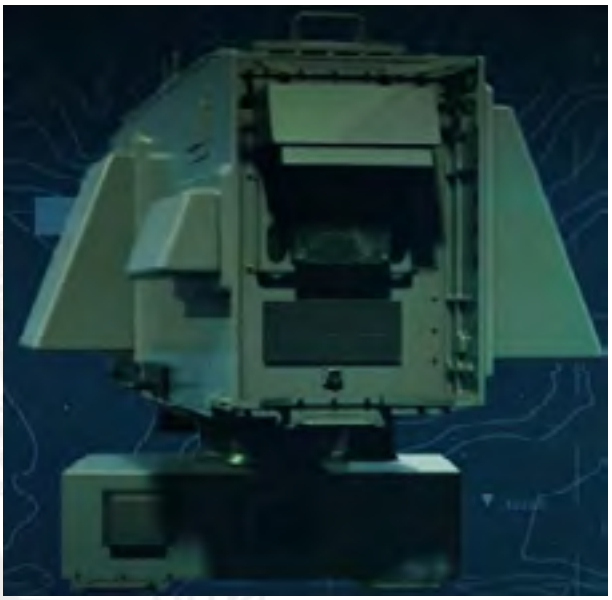
Presenter's Details:
Telangana Police
Zen Anti-Drone System (ZADS)

Features:

- Multi-sensor counter-drone system integrating radar, RF sensors, and EO/IR cameras for comprehensive detection.

- Provides 360° surveillance, AI/ML-based drone classification, and real-time monitoring with command & control integration.
- Equipped with RF jamming and GNSS spoofing capabilities, deployable in fixed, mobile, or portable configurations.

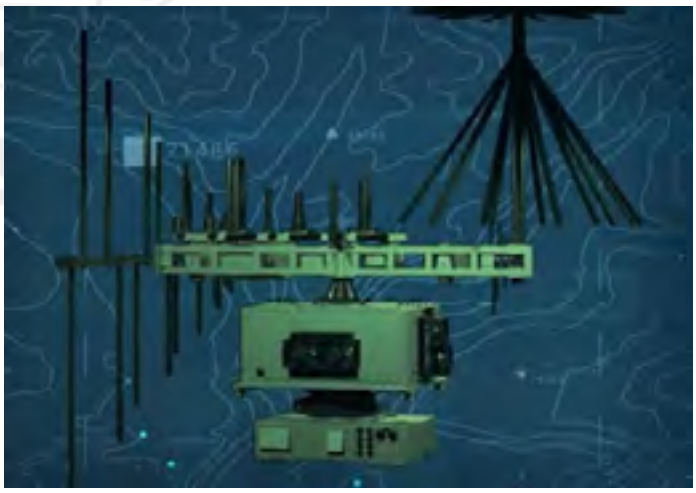
RF Drone Detector



X-Band Radar

Outcomes:

- Enables early detection and tracking of low-altitude and small UAV threats.
- Provides effective neutralization through disruption of drone communication and navigation systems.
- Enhances airspace security around critical infrastructure and sensitive zones.
- Improves situational awareness with integrated multi-sensor data and real-time alerts.
- Supports rapid and coordinated response to drone intrusions.
- Offers deployment flexibility across static and mobile operational environments.



RF Drone Jammer

Presenter's Details:
Zen Technologies Ltd.,

Outcomes:

- Enables rapid detection, tracking, and localization of drone threats.
- Provides effective neutralization of UAV communication and navigation systems.
- Enhances situational awareness for field units in real time.
- Supports quick deployment in urban and high-security areas.
- Strengthens perimeter security against low-altitude drone intrusions.
- Improves response time and operational readiness in counter-UAV scenarios.

Presenter's Details:

DRDO – Defence Electronics Research Laboratory (DLRL)

In collaboration with **Unistring Tech Solutions & Triaitec**

Handheld RFCDS

Portable RF Counter Drone System (Portable RFCDS)

Features:

- High-power tripod/vehicle-mounted counter-drone system for wide-area detection, tracking, and neutralization of UAVs.
- Operates across 400 MHz – 6 GHz + GNSS bands with 360° coverage and AI/ML-based drone.
- classification.
- Provides extended RF jamming (5–8 km) and GNSS disruption/spoofing (3–6 km) with AC power + battery backup support.

Outcomes:

- Supports flexible deployment on vehicles or fixed tripod setups for diverse mission scenarios.
- Enables wide-area surveillance and drone detection.
- Provides long-range disruption of UAV control systems.
- Enhances security of critical infrastructure and sensitive zones.
- Supports handling of high-altitude and coordinated drone threats.
- Strengthens overall airspace security and counter-UAV capability.

Presenter's Details:

DRDO – Defence Electronics Research Laboratory (DLRL)

In collaboration with Unistring Tech Solutions & Triaitec

Portable RFCDS