CONCEPT NOTE ON POLICING IN SMART CITIES

With the increasing demographic shift to urban centres, it is important that the urban landscape and its functional ecosystem are ready to bear with the spurt in population, economic activity and the system inter-dependencies that are going to be concomitant with the urban growth. To meet the challenge of creating efficient processes that are future-ready, citizen-friendly, scalable, replicable and robust, it is important that the systems are smart, logic-driven, self-improving and intelligent. All these aspects are covered under the Smart City concept, which the government has been implementing at a pan-national scale. The 'Smart City Mission' was launched by the Hon'ble Prime Minister on 25.06.2015 in furtherance of the objective of creating modern urban centres that can meet the expectations of the urban dwellers in the 21st century.

From the perspective of public services, the important elements of a Smart City involve:

1. Citizen-friendly and efficient delivery of public services.
2. Proactive resolution of public issues and grievances.
3. Self-improving processes and systems in terms of efficiency, robustness and resilience.
4. Minimal interference and inconvenience to the citizens in their day-to-day pursuits.
5. High adaptability to new technologies and processes with the objective to perform a leadership role for other urban centres.

Since policing is an important service that the state provides to its citizens, hence, in a smart city, the service delivery in respect of police-related services such as citizen-safety, public order maintenance, criminal

investigation, information security, etc. are also required to be aligned with the smart city concepts enumerated above. However, unlike other citizen services and their delivery to the public, policing faces several challenges in a smart-ecosystem, and many of these challenges stem from the very technologies that are so integral to the smart city processes and systems. Thus, for example, the digitisation, automation and the integration/convergence of all systems and processes, while making the systems more efficient, also, at the same time, increases the digital security vulnerabilities of such systems. Further, the integration and the inter-dependencies, while reducing duplication and improving decision-making, also makes the systems susceptible to sudden, large-scale collapses due to cascading effect of minor system breaches.

Further, as it could be made out, the smart cities, due to their intrinsic nature, will be data driven. Thus, data of various parameters will be captured at multiple functional points for the purpose of intelligent, efficient operation of the smart city. This data will also include inputs on individuals' biometrics, location data (personal devices, vehicle, etc.), transaction (financial, social) data and individuals' behavioural data. The smart city systems will be teeming with such data and it is important that the law enforcement agencies undertake the following activities in respect of this data:

- Firstly, it is important that the Law Enforcement Agencies (LEAs) ensure that this data is secured and protected, in view of its privacy implications.
- Secondly, the data, at the public (statistical) level, is utilized by LEAs for efficient emergency response, for proactive interventions in issues related to public order & traffic management and for preventive policing.

- Thirdly, at the level of direct and specific intervention, the data may be utilized for action against desperate criminal elements (persons with past history of repetitive, violent crimes), absconders, POs, and for tracing missing persons, stolen vehicles, smart devices, etc.

The above template of policing in a smart city will require a combination of policing infrastructure for data capture and collation, data integration, data analytics, output-data dissemination, response setup, feedback capture/collection, etc. This has to be supported by an R&D setup comprising of data analysts, research fellows and an incubation centre, for testing and adapting new technologies for policing roles.

Thus, the broad components of a smart city police setup may be as follows:

a. A city-wide surveillance and monitoring setup comprising of CCTV cameras, field sensors (RFID, gun-shot, etc.)
b. An enterprise-level intelligent database integration setup to enable all smart city systems and databases to share data and draw intelligent linkages.
c. A database analytics engine to process multiple databases and live data from multiple feeds for real-time generation of actionable inputs.
d. A setup based on machine learning, deep learning and AI for making the data analytics and decision-algorithms self-improving.
e. A setup for extracting data from open sources and for harnessing crowd-sourced inputs. Community policing in a smart city could be undertaken through community groups on social media, group-messaging applications, civic amenity Apps, etc. The data generated through community policing initiatives should be integrated with other databases for generation of actionable intelligence.

f. An intelligent traffic management system for dedicated handling of vehicular traffic data feeds, analytics, response systems, etc.
g. A central command, control and coordination centre for bringing all the above components under one roof for better functional coordination, especially of response systems.
h. A dedicated data network with built-in redundancies for transmission of data (input/output) captured and generated in respect of the law-enforcement processes within a smart city. The dedicated network is essential for ensuring security of the private data of the citizens captured in course of policing activities and also for ensuring system robustness, especially for emergency response functions and during maintenance of public order.
i. An Information Security/Cyber Security setup for ensuring security of the databases, applications and tools that form the backbone of the smart city intelligent decision making system.
j. An Incubation & Adaptation Centre for studying new technologies, analysing them in respect of smart city policing requirements and if found promising, customizing and adapting them to smart city policing tasks.
k.

The specific components that will cater to the above requirements are:

I. City Surveillance and Monitoring System – Public CCTV Surveillance System
II. C4i and Emergency Operations Centre (EOC)
III. Intelligent Traffic Management System
IV. Cyber Defence Directorate
V. Police Cyber Highway

VI. Incubation & Adaptation Centre / Technology Cell

VII. Community Policing

A. City Surveillance and Monitoring System – Public CCTV Surveillance System

I. INTRODUCTION

a. The modern urban landscape of any metropolis is a buzzing labyrinth full of people on the move with their vehicles and gadgets, and engrossed in their various pursuits. While doing so, people generate tremendous amount of data, which if collected and analyzed, could help the smart cities in becoming more efficient, people friendly, safe and secure.

b. Nothing exemplifies this concept better than the very popular Google application, the Maps. Thus, by intelligently using the GPS feeds from hand-held devices connected to the internet and on the move, esp. from mobile phones, Google Maps creates applications and use-cases that help users find the fastest route and also inform them about traffic congestion, delays, road-blockades, etc.

c. Thus, smart city-wide surveillance and monitoring can help in policing by ensuring efficiency, ease of usage and safety in the ever-increasing chaos of urban systems.

II. City surveillance & monitoring shall be based on the following **broad principles/ paradigms**:

a. It should be dynamic, intelligent and a self-improving system.

b. The system should ensure privacy of common citizens through well-defined protocols for data capture and its access.

c. The system should aid and assist the existing systems through technical interventions by improving efficiency, reliability, speed & appropriateness of responses.
d. The system should lay adequate emphasis on proactive problem-solving for effective redressal of grievances.

III. MAIN COMPONENTS

a. Any city surveillance & monitoring system shall comprise of the following **broad components**:
    i. Video surveillance of public places
    ii. Monitoring of vehicular movements
    iii. Capture of information available in public places – for person identification, vehicle identification, event identification, movement identification, utilities status, etc.
    iv. Capture of behavioural inputs for identification emerging and potential areas requiring intervention.
    v. Creation of databases for all relevant information concerning activities in public places.
    vi. Analysis of real-time inputs received from city-wide input devices in respect of databases, patterns, etc.
    vii. Response system and its integration with city surveillance and monitoring.
    viii. Self-improving decision-making system based on machine learning and AI.

IV. POINTS FOR CONSIDERATION

a. The city surveillance and monitoring systems shall have a dedicated Wide Area Network to link the various city-wide input devices – CCTV cameras, sensors, etc. – with a central facility.
b. The city administration – Municipal bodies, police, transport authority, etc.- has several existing databases such as Utilities' user database, Vehicle Registration & Driving License database, CCTNS, traffic challans, jail release database, etc.
c. A database integration facility to intelligently link all databases relevant for city-wide surveillance and monitoring is important for any city wide surveillance & monitoring system. These include among others, data on crime & criminals, vehicles registration data, live traffic feeds, demographic data, etc.
d. An open source intelligence collection and monitoring tool (OSINT) for getting relevant data from openly accessible databases will allow for feeds from openly accessible online databases, esp. social media, blogs, etc. These databases are very contextual and contemporary and are of great help in identifying trends affecting city administration.
e. A data analytics facility to derive intelligent linkages between the various databases including open source, and also between the databases and real time inputs received from field devices will augment the efficiency and accuracy of the responses generated out of the city-wide surveillance & monitoring system.
f. An intelligent feed analytics facility which is based on machine learning will help in identification of actionable inputs from feeds received from field devices.
g. A facility for integration of the actionable inputs – field device inputs & overlaid data – with the emergency response systems,

such as PCR Vans, ERVs, CATS, etc. is essential for putting the entire system into action.

h. The **salient features** of the proposed City surveillance & monitoring system are :-

   i. Real-time generation of automated alerts and actionable inputs after processing live feeds from field devices in conjugation with various databases.

   ii. Ability to add more use-cases to the system by adding additional data types and/or field devices. The WAN and the analytics engines shall be scalable to incorporate additional use-cases.

   iii. Self-improving decisions making, based on machine learning through intelligent assessment of input feeds, response accuracy, relevance, etc.

II. C4i and Emergency Operations Centre (EOC)

A. The C4i of a smart city will be the central facility where all the inputs such as CCTV feeds, ANPR feeds, sensor data, emergency helpline feeds, SoS App feeds, LBS data, CCTNS and other crime-criminal databases, will get integrated in a functional manner to ensure smooth coordination in performing policing functions. The C4i will ensure the following:

   a. 24 X 7 CCTV surveillance of public places.
   b. Integration of location-based services and crime & criminal databases with real-time CCTV and other feeds for prompt and effective resolution of public safety issues at public places.
   c. Real Time Video Analytics based on AI and Machine Learning for generation of actionable alerts for preventive and curative response.
   d. Use of Video Analytics Tools: Facial Recognition System and Number-Plate readers for real-time tagging of crime & criminal information with specific time-stamped video feeds.
   e. Multi-tiered Command, Control and response set up at PS level, District level and Police Hdqrs. level for effective information sharing, planning, decision making and execution for prompt resolution of public safety related distress situation.
   f. Provision of Emergency Operation Centre (EoC) integrated with C4i as a dedicated Command Room to attend to individual public safety issues of serious nature.
   g. Integration with crime & criminal databases: CCTNS, Criminal dossier system, e-Challan system, JAIL release, JAIL visitors etc. for effective real-time analytics, suspect tagging and alert generation.

h. Integration with Emergency Response Support System (ERSS, Dial 112) for real-time inputs on public safety related emergency calls.

i. Integration with location-based services envisaged under ERSS for identification of exact location of public callers in distress (on demand).

j. Location based CCTV feed sharing with field units: Police patrol vans, Police Station Emergency Officers, beat patrolling staff, Emergency Response Vehicles, etc. involved in redressal of public safety related distress situation.

k. Integration with Himmat SOS Mobile App. for real-time inputs from women in distress.

l. Audio Visual feed aggregation from relevant on-ground sources – Private/Public IP based CCTV systems, etc. mapped over the C4i GIS application, Mobile-camera feed of Himmat App. Caller – and their real-time sharing with a ground staff tasked with redressal of distress-situation affecting a smart city resident in a public place.

B. The CCCC Centre (C4i) in a smart city should have these broad components:

a. Interactive Video Wall with intuitive GUI.

b. A high capacity database storage facility

c. Database Integration Facility for bringing all existing policing databases on common platform

d. A high-capacity data analytics engine with AI/ML capabilities

e. Integration with ERSS, LBS and SoS Applications

f. OSINT tool

g. Picture Intelligence Unit for dedicated collection of PoI pictures from open source.

III. Intelligent Traffic Management System

One of the pre-requisites of a smart city is availability of an efficient commuting system that provides end-to-end connectivity through reliable, comfortable, safe and affordable means.

The vehicular traffic in a smart city may be characterized by the following:

i. Extensive usage of MRTS
ii. Hub-and-spoke model involving MRTS, with cluster buses (preferably electric buses), e-three-wheelers, and bicycles-on-rent for last-mile connectivity.
iii. Pedestrian friendly roads and traffic regulation systems
iv. Multi-level and underground parking for private vehicles
v. Premium on usage of private vehicles in designated areas and during designated times, etc.
vi. Introduction of intelligent vehicles, followed by self-driven vehicles.

Thus, a smart city will have all the essential elements of a traffic system that only needs an intelligent management system to ensure its smooth operation. The intelligent traffic management system in a smart city may comprise of:

1. Sensors on roads for monitoring traffic density, flow, etc.
2. Intelligent traffic signal management based on AI/ML for minimizing traffic built-up, clogging, waiting-time and for ensuring efficient utilization of road-space, alternate routes, etc.
3. Interface between an individual's route preferences and traffic signalling systems for real-time traffic guidance and traffic optimization.
4. ANPR Cameras, RFID scanners, sensors, etc. for traffic prosecution.
5. Virtual lane marking and lane discipline through smart car controls.

6. Smart traffic solutions for self-driven vehicles, including virtual signalling systems, virtual lanes, vehicle-clustering (for efficient bubble movement of vehicles moving towards common destination points/routes), etc.

In this regard, it is important that the civic authorities in Smart Cities constitute a Task Force or a Working Group that periodically monitors traffic flows, bottlenecks, public feedbacks, AI-based improvement suggestions, etc. and takes prompt action in resolving traffic-related issues. In this regard, it is important that the Head of the Traffic Police Unit as well as the road-building and maintenance agencies (PWD, MCsD, etc.) are given due representation in the Working Group.

IV. Police Related Citizen Service Delivery ina Smart City

In a Smart City, it is important that the citizen avails public services with utmost ease of access, with adequate information about service choices, service terms & conditions, service deliverables/outcomes and service quality, and is assured about the fairness and truthfulness of the public services rendered. The citizen also expects a proactive management of the service outcomes and the citizen's satisfaction level through sustained follow-ups.

Thus, the essential requirements of a service delivery model that is likely to conform to these criteria are:

i. A standard, well defined service delivery system with objectively stated outcomes.
ii. A standardized flow-chart of various steps involved in the service delivery, their input requirements, their outcomes/deliverables, time durations, etc.
iii. Minimal subjectivity and human intervention in the service delivery decision making.
iv. Feedback capture and its utilization in improving response accuracy and efficiency.

The policing related services should also be delivered in a Smart City as per the above proposed model. For instance, the most important service delivery done by LEAs is 'Registration of FIR and Investigation of Cases'. In a Smart City, the delivery of this service could be made through AI based Intelligent Complaint Registration Application hosted over the Internet or through smart, physical interfaces. This application may utilize Natural Language Processing, speech recognition and deep learning to identify sections of law, jurisdiction, etc. while registering a formal FIR. Such a tool will drastically reduce the human

factor in the delivery of a very critical service, and by doing so, help curb attain standardized, truthful response, equal access and other benefits to the citizens. The LEAs operating in a Smart City should strive for developing more such tools for citizen service delivery.

V. Crime Data Analytics

Law and Order management is a prerequisite and an essential condition for the working of a smart city. Technology has, today, pervaded all aspects of life bringing upon new challenges for law enforcers. In this context, it is imperative that police evolves in an organic and holistic manner to face these challenges.

In this regard, new technologies, from robust surveillance systems to predictive algorithms, are transforming the law enforcement today. The development and dissemination of such new crime-fighting tools is rapidly increasing and in this post-modern narrative, being the police organization of a smart city, any police force will need knowledge management systems and models while dealing with real time data and big data to enable itself to make an informed decision to cater to any eventuality.

PROBLEM ARENA AND NEW AGE PARADIGM:

With the evolution of society, the new challenges being faced by police in law and order front are the issues of unregulated, motivated and flash mobs. Butterfly principle prevails wherein some incident in one part of the globe can cause unrest in other part of the world, induced by social media or otherwise. Adding to the issue of prediction is the inability of intelligence sharing in real time and also the purview of compliance of human rights. On crime prevention and detection front, especially the intelligence collection side, technology can play a tool in ensuring better predictive and evidence based policing.

TECHNOLOGY AS A SOLUTION:

- **SOCIAL MEDIA MONITORING AND ANALYSIS**: Today, social media has become a major tool for creating propaganda, connecting and mobilizing mass

movements. It is imperative to supplement the traditional policing with social media monitoring tools which keep a tab on pulse of the netizens and generate red herrings wherever required. The department of Homeland Security in USA uses such tools to analyze people who are vulnerable and to counter violent extremism by keeping tabs on any sensitive information via keyword surveillance. Along with the analysis and detection, the tools will also focus on correcting / clarifying the misrepresentations in circulation on social media.

- **USE OF VIDEO SUVEILLANCE WITH AI COMPONENT AS MAJOR PART**: With the advent of the culture of flash mobs and unregulated unrests, the effective monitoring of the public, especially the movement as well as the identification has become a limitation without the scientific aids. It is therefore needed that in a smart city, the CCTV Cameras network be integrated with the C4i in PHQ to monitor the individuals involved in organizing and participating in such crowds. Further, the Police can use body-worn cameras to create a video pool of information of such participants. These body-worn cameras also serve as a deterrent in managing law and order. Use of surveillance drones can also be emphasized upon for aerial surveillance which will serve the same purpose. Further, the drones provide additional maneuverability in blind spots to keep more effective check in law and order maintenance. In this regard, it is pertinent to mention that a successful integration with all stakeholders storing data is required to generate real-time action points, but this has to be done under a very strict protocol for retrieval of this data. Preventing misuse of this data and taking care of privacy issues will be a challenge for a smart city police in future.
- **ARTIFICIAL INTELLIGENCE TOOLS AS A FORCE MULTIPLIERS**: Use of facial recognition, sentiment analysis and audiovisual fingerprinting to analyze

the pool of audio and video data collected to predict the crowd behavior as well as in identifying the miscreants/ repeat offenders. San Fransisco based Deep Science AI has developed Artificial Intelligence Surveillance (AIS) platform which uses deep learning to identifying real people concealing their faces/ firearms of intruders after-hours or where they shouldn't be, and alert a security analyst monitoring remotely. AI based cameras with the help of facial recognition and gait analysis technologies can also be used to suspect anomalies like unattended bags, suspicious crowd behavior etc.

- **USE OF FINANCIAL ANALYSIS TOOLS:** Tools are required to keep a track on suspicious financial transactions taking place online or over the dark web which is used to sponsor and organize mass protests. It is a known fact that various organizations and vested interests attempt to destabilize the economies and create social unrest through sponsoring protests. To counter such efforts, FIUs should be integrated with policing systems and all transactions from identified individuals be kept a track upon.
- **TRAFFIC MANAGEMENT:** Traffic patterns are highly unpredictable and movement of vehicular traffic and heavy goods is subjected to a great degree of uncertainty. By the use of AI, IR maps can be generated to create a model to allow management of traffic lights in such a way that prior to buildup of traffic either planned (Rush hours, VIP Routes) or unplanned (accidents, water logging etc) alternate routes can be opened up and traffic can be redirected to those routes. In addition they can also act as gateways for lifesaving ambulances and police vehicles to choose the most efficient path to reach a place of occurrence/ scene of crime.
- **INTEGRATION OF BEATBOOK WITH CCTNS**: Delhi Police has a very robust beat policing system in which every beat officer maintains a comprehensive

data of demographic information of their beat. This system can be integrated with the CCTNS to create a nationwide database. It can be effectively used for real-time verification of information sheets (Register no.12), real-time information sharing in a holistic manner in a smart city policing setup.

- **USE OF BIOMETRIC TOOLS:** Through a network of both online and offline methods, biometric data such as fingerprints, facial and iris characteristics can be fed into a system to identify and create a working model for the back end to identify a particular person. This is efficient in tracing missing persons, absconders and potential movement of criminals across borders. In this regard various tools have been developed to supplement the efforts of police.

USE OF AI FOR CRIME PREVENTION: AI deep learning models coupled with crime mapping can be developed to analyze crime patterns and identify hotspots which act as a useful tool for predictive and preventive policing. Context-intelligent image analysis deep learning model can help identify networks through which sensitive data passes thereby reaching the perpetrator. There have been instances wherein such tools have been used effectively in cases of human and child trafficking by monitoring the networks at the telecom operator levels. There is a need for creating a nationwide database of criminals under various categories, which can aid the police in developing localized crime prevention strategies. In various countries, databases of sex offenders/ human traffickers/ drug peddlars etc serve the similar purpose. To check the interstate crimes, Integrated Prison and visitor records from CCTNS clubbed with AI based machine algorithms can aid the police in monitoring the

activities of criminals across India. Use of satellite imagery can help a long way in metropolitan policing.

AI based on algorithmic software can also be used at the crime scene for immediate recognition of perpetrator based on modus operandi, pattern of crime/criminals in the area, biometric data, forensic data etc.

- **CREATING FLAWLESS CHARGESHEETS:** AI has tremendous potential to create paperwork which today is done manually. A machine-learning algorithm can generate charge sheets specific to an incident with complete legal validity without any exclusions or non-conformity. This allows minimal manual intervention hence the scope for malicious intent is not there in any way and the ability of the legal system to prosecute to the fullest extent of the law is always available. In the charge sheet, references from other judgements as well as other outcomes can also be included to make it more effective. Today, most judgement level analysis has already moved to Artificial Intelligence based systems with zero manual intervention. It has been proven that AI based systems have outperformed lawyers as well as judges in some cases. A neural network based system over a period of time can also create sensor based inputs in order to predictively allow for the analysis of outcomes of cases as well, helping speed up the judicial process. The consequent burden on the policing system goes down.

VI. Cyber Defence Directorate

Information and its flow will be the lifeline of a Smart City. It is important that this lifeline is secure, protected and shielded from external and internal attacks. For this purpose, it is important that a dedicated Cyber Defence Directorate is established under the police leadership with the mandate to ensure cyber security of the Smart City and its institutions and to protect the citizens of a Smart City from cyber crimes.

For this purpose, the Cyber Defence Directorate of a Smart City Police Force should comprise of:

i. Emergency Operations Centre for 24X7 watch over the critical IT infrastructure of the Smart City.
ii. Cyber Security Centre for enforcement of information security policies across the various entities of a Smart City. This centre will work on the principle that a chain is as strong as the weakest link. Thus, the Centre will strive to strengthen each and every entity of a fully connected and integrated Smart City.
iii. Cyber Crime investigation Unit – for scientific investigation of complex cybercrimes that are likely to target institutions and residents of a Smart City. Action against cyber criminals is important to instil confidence in the digital backbone of the Smart City governance model.
iv. Cyber Awareness Unit – for keeping the residents of a Smart City well informed about the various cyber threats and the safe online habits needed to protect oneself from these threats.
v. Cyber Intelligence Unit – The cyber space, by its very nature, is such that it can be accessed from anywhere across the globe. All that is required is appropriate credentials. Thus, cyber space is very conducive for

intelligence collective and proactive interventions. In a Smart City, since there will be zero tolerance to system breakdowns, hence it will be imperative that the police agencies engage in proactive handling of cyber threats and their effective neutralization. The Cyber Intelligence Unit with participation from multiple stakeholders will help in attaining this objective.