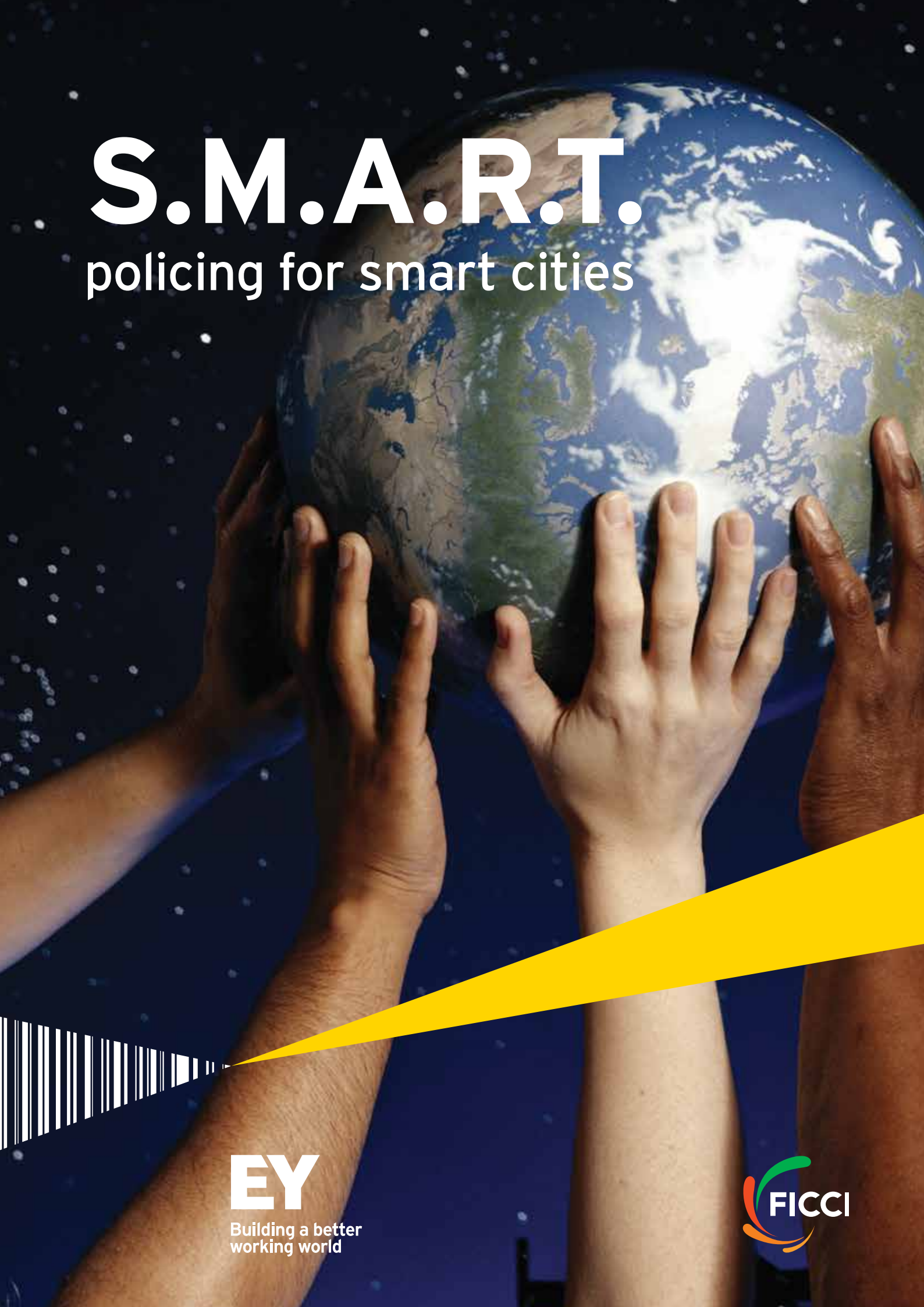

S.M.A.R.T.
policing for smart cities
EY
Building a better working world
FICCI

Foreword

Cities have always faced challenges in their functioning and operations. With the increasing complexity of IT infrastructure, applications and networks, the challenges have risen far and beyond. Securing these cities is an increasingly formidable task.

In general, the size of a city and its crime rate are directly correlated. The cost implications of criminal activities are significant. And the avalanche effect of a small attack can lead to larger issues in the integrated smart city. The risk is not only in physical form but can also affect the citizens emotionally, socially and economically.

Smart cities need to address the challenges using S.M.A.R.T. police force, which can prevent accidents, emergencies as well as crime. Smart police is a modern police that can relate to the citizens of a smart city and can also act efficiently using IT enablement. Smart police should be capable of protecting the city's physical and IT infrastructure. Minimum response time is expected from smart police in case of an emergency. The police also needs to make efforts to recover the city from any major incident. In order to help citizens in all aspects, the police needs to be smart and agile.

Through this paper, we have discussed the concept of S.M.A.R.T. policing. It is an attempt to highlight the capabilities required for policing a smart city. I sincerely hope that readers benefit from the S.M.A.R.T. police concept discussed in this paper and appreciate the kind of policing required for the new smart cities.

Rahul Rishi,
Partner, EY

Foreword

Modern cities are witnessing integration at various levels, and thus the need for a modernised, integrated and secured system. The requirements of the modern police forces have been appropriately captured by honourable Prime Minister Shri Narendra Modi in the word "SMART". He emphasised that a professionally efficient, technologically enabled, socially sensitive police upholds the rule of law and human rights in all situations and is also engaged optimally with the community.

India is the one of the fastest growing economies in the world. Along with this economic growth there has been an exponential growth of population in cities and metros. In order to maintain this esteemed position we should thus focus on maintaining safety and security of our citizens, businesses and critical infrastructures. India will have 100 smart cities in the coming years. SMART policing is thus an essential requirement. This has become all the more important in the light of increase in organised crime in urban spaces and the growing nexus between terrorist organisations the world over. Given the advancement in technology, the future of internal security and policing infrastructure lies in better use of data and information for pre-emptive policing.

The FICCI-E&Y report on SMART Policing for Smart Cities explores the possibility of shifting from traditional police systems to a SMART policing structure. The report explores in depth India's policing architecture, and compares and correlates best practices from around the world. It analyses various components of analytics and intelligence required by modern enforcement agencies, and underlines initiatives that need to be taken for the transition. It further highlights the use of modern technology in solving important and complex security issues of the country. I sincerely hope that this report will offer important and useful insights to the government, enforcement agencies and all other stakeholders.

Dr. A. Didar Singh
Secretary General, FICCI

Contents

1. Executive summary

"By 'SMART' policing, I mean
S for strict but sensitive,
M for modern and mobile,
A for alert and accountable,
R for reliable and responsive and
T for techno-savvy and trained."

- Narendra Modi, Prime Minister of India

The words of India's Prime Minister reflect that the country is looking to move toward SMART policing from the traditional ways of policing. Efforts have been made by multiple states and union territories to adopt new methods of policing.

Smart cities are constantly evolving with connectedness in cyber space between people, buildings, transport, energy, water, communications, commercial operations, media and the multitude of activities cities generate. The boundaries of smart cities are in cyber space, which creates global linkages in the connections to systems. This brings in a different threat horizon that has to be monitored for business operations, safety and continuity of activities. Cyber events — whether accidental from failures to integrate rapidly changing technologies or intentional from individuals, terrorists or nation states — are rapidly creating disruptions and uncertainty.

The threats so created in smart cities impact citizens physically by affecting the infrastructure and the health of the citizens themselves. They can have economic impact in case of frauds, or attacks on utilities such as power and water. Attacks can also affect citizens emotionally as many things can be lost to the attack. An attack can even be made to the culture and society as a whole. There are risks to all business processes that are impacted with the failures of systems delivering these business processes within intelligent buildings and to the world through cyber space.

A quantified risk analysis across the smart city risk horizon can support safety, security and environmental management, and reduce the levels of uncertainty that confront business and government operations every day.

S.M.A.R.T. policing is an attempt to explore the risks associated with policing in smart cities. A new way of policing is defined through a set of five principles – strict and sensitive, modern and mobile, alert and accountable, reliable and responsive, techno-savvy and trained.

Strict and sensitive: This principle emphasizes the partnerships that can achieve long-term benefits for the police force. Police force needs to be strict while enforcing the rules of the land while being sensitive to the social sentiments of the general public. The understanding of social sensitivity can be further enhanced by partnership with society.

Modern and mobile: Police needs to increase its outreach and efficiency by adopting newer technologies and means of mobility.

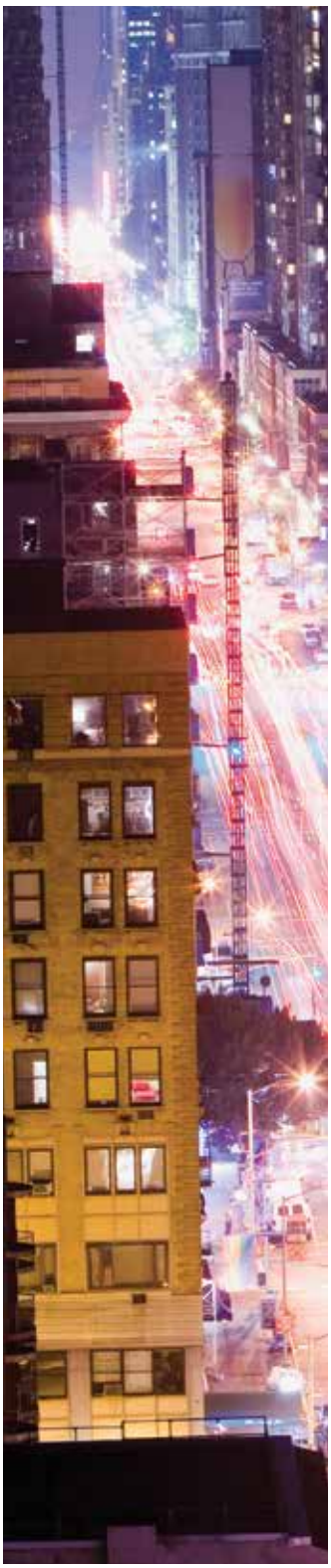
Alert and accountable: Alertness can be increased by strengthening intelligence network and in-depth analysis of information gathered. Additionally, partnerships with the society to have more eyes and ears on the ground will improve the alertness about the day-today activities in neighborhood. The smart police have to be accountable to citizens and to the government for its actions.

Reliable and responsive: In smart cities, police needs to be more responsive and should act on any input information from various mediums such as phone calls, emails, IoT devices, panic buttons, etc. With improved responsiveness and effective actions, reliability on police increases dramatically.

Techno-savvy and trained: This principle highlights utilizing modern IT applications that are more accessible by public. This helps the police in crowdsourcing data through the public and increasing the intelligence in case of attack. The police needs to be trained enough to analyze and make use of the information collected through various means.

Recommendations from the "Policy Roundtable - SMART Policing" enrich the S.M.A.R.T. policing principles. They provide a way forward for Indian state police forces to become smart for smart cities.

02 Defining smart cities with smart police



The ability of technology to drive dramatic productivity improvements in an economy is now well-established. With technology continuing to become smarter and cheaper, the application of ICT solutions has also grown. Today, we are increasingly able to create, manage and store large datasets – or "big data." We can collect data that makes it possible to track and predict the behavior of people and systems in ways that were not possible just a few years ago.

Policing has been around for centuries and the tasks of police have not changed much over the millennia. The growth in policing can be seen in three stages:

1. **Informal policing,** where all members of a society equally share the responsibility for providing protection and keeping order
2. **Transitional policing** occurs when police functions are informally assigned to particular members of the society
3. **Formal policing,** where specific members of the community assume formal responsibility for protection and social control

With the growth of smart cities, policing has also evolved in the past years. This chapter showcases the brief journey of how police evolved.

Traditional policing

In early historical times, there were people to ensure the safety of citizens and property, but a well-organized police force does not seem to have existed. There is no portrayal of warfare in the Harappan civilization, nor have good weapons such as spears and swords been found. However, it is believed that the Harappans had some form of armed police to protect the public and deal with criminals. In ancient Egypt, early guards and watchmen may have been, at least in part, purely local answers to security concerns. They may have been employed by private persons and local institutions such as temples or rich landowners. During the Middle and New Kingdoms, however, a nationwide police force grew out of the semi-military units securing the borders.

As the population increased and crime began to rise, steps to improve policing were taken across the world. From 1066 to the 1300s in England, police services were provided through the frankpledge system. Under this system, citizens were appointed with the responsibility of maintaining order and controlling crime.

During the 1700s, the foundations of modern policing were laid. The Bow Street Runners in England was the first group paid through public funds that emphasized crime prevention in addition to crime investigation and apprehension of criminals. The group added a new dimension of preventing crime through preventive patrol in the traditional policing methods..

Modern policing

With the passage of time, population increased and so did sophisticated crimes and criminals. Blue collar crimes, profit-driven crimes and organized crimes rose in the 20th century. The focus of policing was not only to prosecute the individual but also to prevent the crime. Efforts were made to provide Information, Communication and Technology (ICT) solutions to the police force and significantly increase their efficiency.

A range of technologies is used to gather, store, retrieve, process, analyze, and transmit information. Relevant ICT may range from systems installed in public environments over PC-based systems in offices, to systems installed in cars and mobile systems used on-site. In addition to systems that are specifically designed for the police, ICT in use by the general public may offer the police new means of carrying out their tasks.

Modern policing includes the use of CCTV surveillance, radio frequency identification, e-identification, online verification for passport, etc. Modern police is dependent on ICT systems to be more efficient and effective.

The degree of city security, measured in terms of the security of intellectual, social, technical, environmental, cultural, leisure and financial capital, can be based on crime, disaster and accident; all of which can be of internal or external origin. Challenges across the stages of modern policing in India are:

Mitigation planning	Preparedness	Communication and response	Review
▶ Lack of security & surveillance in cities ▶ No integrated baseline database of crime and disaster ▶ Difficult to track records ▶ Limited use of modelling/ prediction tools for trend and risk analysis	▶ Limited tools and technologies such as forensics, analytics, early warning systems, disaster web page etc. ▶ Lack of integrated database of various sectors like banking, telecom etc. ▶ No dedicated network for information distribution	▶ Limited use of GIS tracked vehicles, mobile command and control vehicles ▶ Limited logistical support option for providing relief materials, damage surveys, baselines amps, equipment, human resources and funds ▶ Limited special access capability post disaster	▶ Difficult to archive and share knowledge ▶ Limited post case analysis ▶ Difficult to manage data

Smart policing

Every year, the UK's Metropolitan Police spends around £250 million on running its ICT, most of which is used to maintain outdated, ineffective and overly expensive systems. Smart policing can be defined by the use of modern technology and processes, which increases the efficiency and effectiveness of the policemen on the field. It should include real-time data, social media communication, field tablets, predictive policing tools, and several other options.

Smart policing is important in cities of future, i.e., smart cities. The smart cities can be defined by the presence of smart infrastructure including smart grids for power and water, effective waste disposal mechanism, green transport and modern policing methods. Smart cities extensively use ICT for all services and provide seamless transactions to citizens from one department to other. Greater ICT usage increases the risk to citizens' information, governments' data and business' plans. In a smart city, policing is not limited to safeguarding infrastructure but also includes safeguarding data and information.

03 Smart cities and their security risks

Smart cities are going to be the reality for municipalities around the world. These cities will use communication networks, highly distributed wireless sensor technology, and intelligent management systems to solve current and future challenges, and create new services. The key features of smart cities can be defined as:

a. **Smart governance:** Flexible governance structure, technology enabled decision mechanisms, smart regulation to connect city laws to new digital realities, and innovation clusters to create jobs and vibrant economies

b. **Smart economy:** Viable and sustainable business opportunities and the presence of innovative enterprises, clubbed with quality education and infrastructure to provide better economic status to the city

c. **Smart environment:** Management of waste disposal in cleaner ways, maintaining pollution free air, water treatment plants, etc., to provide a cleaner and greener environment to citizens

d. **Smart living:** Technologies to integrate and analyze massive amounts of data to provide better living to citizens in the form of childcare facilities, community libraries, entertainment modes, hospitals according to area needs, etc.

e. **Smart people:** Services, notifications, and information to citizens, such as where to find a parking spot or a new local shop or even to monitor air pollution; connect citizens to local government and encourage more direct participation, interaction, and collaboration

f. **Smart mobility:** Extensive and efficient public transportation network, park and ride, diffusion of ecological cars, limited traffic areas, cycle paths, bike and car sharing

The ecosystem of smart cities can be viewed as below.

	Social, Corporate, Government and Academic Communities	
	Smart Government eGovernment Open Data Public Infra **Smart Living** Health Safety Culture **Smart People** Education Inclusivity Creativity **Smart Mobility** Rail Road/foot Air/Sea **Smart Environment** Energy Water Buildings **Smart Economy** Innovation Research Connectivity	
Developing & Enhancing Smart Capabilities	**Interface and Access** | Web Access | Mobile Access | Open Data & API Access |	**Performance Monitoring & Management**
Partner Ecosystem Peer Research & Collaboration Investment Planning & Prioritisation Change Delivery	**Smart Services** | Operational Control | Social, Geo & Contextual Services | | Search, Filtering & Personalised Services |	Benefits Definition Benefits Tracking & Optimisation Reporting & Transparency Rule & Policy Governance
	Intelligent Data Core | External Data Feed Monitoring | Event Processing | | Event Ingestion & Aggregation | Collective Intelligence | Analytics |	
	Instrumentation | Sensors | Infrastructure Control | Data Collection |	
	Core Infrastructure and Networks | Buildings | Energy Grids | Water Network | | Transport Grids | Telecoms and ICT Infrastructure |	

Changing lives of citizens in smart cities

A typical day of smart citizens could look like this. They wake up on a regular working day, take a look at their smartphone or tablet, and explore a mobile app to choose the best route to go to work. They check train, bus and subway schedules. They also check the temperature, pollution level and weather conditions (based on which they make simple decisions such as packing an umbrella or a jacket.

Sensors everywhere are feeding city systems and these are sending the data to mobile apps. Let's say the person chooses to go by car as there was a delay in public transportation. On their way to work, they check a mobile app for the best route to avoid traffic and another app to select parking based on availability and pricing. Traffic flow is good because of smart traffic control systems that adjust traffic lights based on current traffic conditions. Because of rainy weather, smart street lighting will leave street lights on until there is more daylight. If rain causes floods, flood detection sensors will immediately alert the city management and citizens. The city management closely monitors the entire city with the help of surveillance and traffic cameras. The rain causes public transport delays, and information on delays is pushed out so people can choose transport alternatives.

Smart citizens are interconnected via smartphones and gadgets. Smart energy meters, security devices and smart appliances are being used in many cities. Homes, cars, public venues and other social systems are now on the path to full connectivity, known as the "Internet of Things (IoT)." Standards are evolving for all of these potentially connected systems. To benefit from them, city infrastructures and services are changing with new interconnected systems for monitoring, control and automation. Intelligent transportation, public and private, will access a web of interconnected data from GPS location to weather and traffic updates. Integrated systems will aid public safety, emergency responders and disaster recovery.

Smart cities are vulnerable to risk due to their interconnected nature. Attacks can be made to any point of the infrastructure and network. In addition to the primary network, the city data centers catering to the various domains would also be open for exploitation in the event of a security attack. Numerous cyber attacks in the cyber domain have been launched in recent years against the computing infrastructure of various governments. These have been aimed at undermining the functioning of information systems, theft of information, or denial of service. These threats have multiplied in today's networked Internet of Things (IoT) paradigm, where machine-to-machine (M2M) interfaces have increased.

With computing systems, the core of security and privacy concerns is the information handled by the system. The three general areas to be secured are:

a. The "privacy" and confidentiality of the information

b. The integrity and authenticity of the information

c. The availability of the information for its use and services

3.1. Risks in smart cities

Traditionally, risks have been associated with the physical damage caused by the attack. However, with emergence of integrated IT environment, any attack on smart city or citizens of smart city, the attack is not just of physical nature. A modern Indian city embodies people, knowledge, resources, finances, democratic and political aspects, and cultural values. These constituent elements can be classified as asset groups or capital, including intellectual, social, technical, environmental, cultural, leisure and financial capital. Attack can be made on any constituent of the city and can impact socially, economically and emotionally in addition to physical damage. Different types of risks that a smart city faces are discussed in this chapter.

Constituent elements of city					
Intellectual & Social Capital		Financial Capital	Cultural & Leisure Capital	Technical Capital	
People	Information Resources	Economy	Values & Religion	Natural Infrastructure	Man made infrastructure

Figure: Constituent elements of city

Risks include illegal access to information, and attacks causing physical disruptions in service availability. As digital citizens become increasingly connected with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency responses when needed are technological challenges that go hand-in-hand with the continuous security concerns.

In 2012, the first major case came before the US Supreme Court on instrumented/ interconnected/intelligent systems involved a GPS tracking device. The Court found the placement and monitoring of a GPS tracking device on a person's automobile while it travelled on public roads to be illegal due to lack of sufficient evidence relating the vehicle to criminal activity as determined by a neutral magistrate. This was an "unreasonable search," even though it would have been completely permissible for police agents to follow the automobile in their own vehicle and log the movements.

Although a prevailing rationale was that the placement of the tracking device without permission was a trespass, Associate Justice Sonia Sotomayor, in a concurring opinion, addressed the growing, pervasive risks of computing and communications technologies, such as GPS-enabled smartphone. Electronic surveillance may still be improper "when the government violates a subjective expectation of privacy that society recognizes as reasonable." She agreed with Justice Alito that long-term GPS monitoring would impinge on those expectations.

However, Justice Sotomayor continued in United States v. Jones:

In cases involving even short-term monitoring…GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations…("Disclosed in [GPS] data…will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future…And because GPS monitoring is cheap in comparison with conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." Illinois v. Lidster, 540 U. S. 419, 426 (2004).

The knowledge of such surveillance as referred in earlier example could have a negative impact on freedoms of speech and association with others as well as provide the government with immense private information subject to misuse.

GPS systems can track destination and origin points, and may even store the actual route taken. Access to contact lists and messages can reveal much that may need to be kept private for personal, professional or commercial reasons.

Human factor failures are integrated with technological failures and malevolent events from insiders, organized crime, and nation states intent on disrupting critical operations such as finance, communications, defense and security, media, transport, energy, water and other infrastructure.

Therefore, the smart citizen today is under threat of risk and attack at four levels:

- Physical
- Economical
- Cultural
- Emotional

For the smart city, the technical target and the related consequence, such as injury to property, personality, life and limb, or emotional damage, must be viewed jointly and, in turn, mapped to the nature of the motivated offender.

In the context of transportation systems, motivated offenders may include juveniles, thieves, vandals, stalkers and domestic abuse perpetrators. The motivations range from boredom to malice to profit to insanity. Instrumented transportation systems offer suitable targets for a motivated offender.

First, the victim/target's privacy is heavily compromised because access to vehicle systems provides the offender with near-complete information on where, when and for how long the victim/target has visited a particular location.

This privacy violation is a major security risk. Once motivated offenders have a profile and location on the victim/target at all times, they know when that victim/target would be most vulnerable to a **physical attack.**

Catastrophic failures may also occur because highly connected systems can suddenly fail from a critical point coming under pressure, or from a convergence of operations that create a new central point of weakness or a vulnerable target for malevolent action against the company's or government's operation. New threats to systems controls in smart grid, smart water supply/distribution or smart transportation, etc., widen the threat spectrum beyond data protection and software failures. There are risks from any inability of a facilities management process to access its building control systems or to see the systems data on operation of essential services (energy control, access control, communications, unauthorized devices on the system, unauthorized access across systems)..

Locational data can be a key security concern. Many people set the GPS originating address from their homes. Access to this data reveals that home location. If the automobile is away from home, that home may be a better target for burglary – a case of **economic loss** to the citizen.

Similarly, social media can be used as an amplification platform for attacks. For instance, attackers can increase the impact of an attack by causing panic in a population. If just one simple attack is real, then a bigger attack can be promoted. Even if the promoted attack never happens, it will scare people. Every day that such a problem persists, it will grow and incite increasingly angry citizens and make them **emotionally weak.**

New smart city projects exemplify an increasingly popular phenomenon: new town development through collaboration and co-branding among governments. Unfortunately, many such projects frequently overlook the peculiarities of indigenous **culture** in favor of a commoditized landscape designed to serve commercial interests.

Such projects often support economic goals but may compromise local identity by imposing an inadequately contextualized vision of development that focuses on economic and environmental indicators to the exclusion of **cultural authenticity.**

Cultural heritages are fundamental aspects of our identity and must be transferred to the next generations in the best possible condition. Cities need to make efforts to develop innovative conservation strategies and integration of the most advanced technologies to allow their safe, sustainable and effective use in the context of the smart management of the city.

Bringing people together – Meaningful adjacencies

According to a concept known as "meaningful adjacencies," the names etched onto 76 bronze panels surrounding two memorial pools at the site of the fallen Twin Towers, New York, are being grouped by the victims' relationships with each other. The media design firm that planned the memorial sought help from the victims' loved ones, and roughly 1,200 requests for meaningful adjacency placement were returned. With the help of a software programmer, an algorithm (called Names Arrangement) was created that would arrange the "really irregularly shaped puzzle pieces" built from the adjacencies. The first level of clustering is fairly obvious: firefighters with firefighters, cops with cops, all the members of each of the flights, first responders, or friends. However, beyond that, the groupings become more complex in a way that packs a more "emotional impact." Within these sub-clusters, the names are arranged to reflect friendships and family bonds.

3.2. Countering risks by smart policing

The dynamic, changing threats evolving from design, commissioning, operation and change management stages in such a city all require solutions and risk-based decisions within a coherent and harmonious security framework. They also require evaluation of the threat landscape, the safety, security and integrity of systems and people within this landscape, and how business can manage through uncertainties.

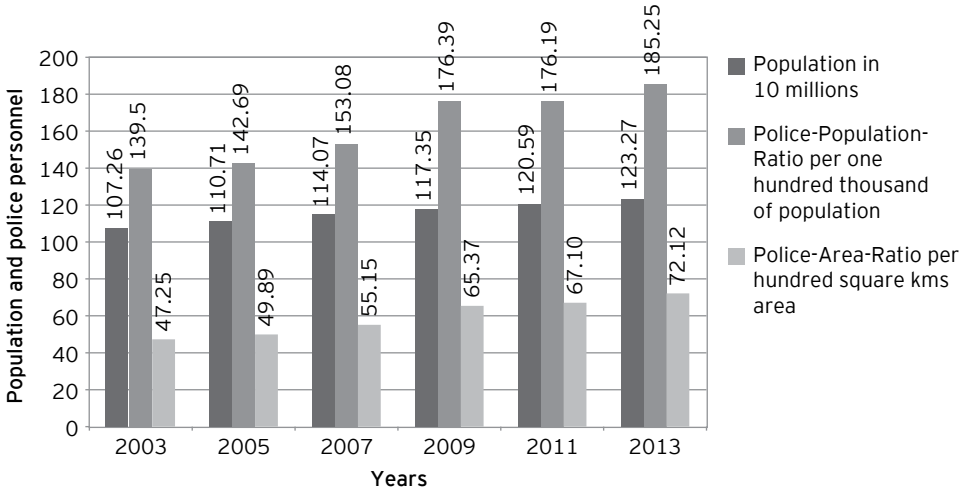
Along with risk assessment, smart policing is an aspect that can immensely contribute to the prevention and control of risks arising from these connected people, infrastructure and systems.

As defined earlier in this paper, cities are at a point where smart policing is more of an imperative than a mere need.

04 S.M.A.R.T. policing

India has seen a growing police force in the past decade. Total population increased from 1072.6 million in 2003 to 1232.70 million in 2013, whereas the police force strength increased from 1.52 million to 2.28 million during this period.

Police-Population per 100,000 of population and per hundred sq km during 2003-2013



Source: Data on Police Organizations in India, Bureau of Police Research and Development, 2014

The increasing trend of urbanization in India is leading to increased vulnerability of cities: terrorist attacks, crime, social unrest and heightened impact of natural disasters are just some of the safety and security issues that need to be addressed. The increased police force faces the challenge of managing cities that are growing rapidly and becoming increasingly complex.

Growing skyscrapers, increased use of public transportation, multi-tenant buildings, and thousands of people flocking together for sports or cultural events mean that large numbers of people are packed in smaller areas in a smart city. Such densely packed areas become soft targets for attacks, as evident in case of the Boston Marathon bombing in 2013, killing 6 people and injuring 280 others.

However, in smart cities, business continuity becomes a greater issue in ensuring the city's ongoing prosperity. The concept of urban security – protecting citizens and infrastructure such as airports, data centers, roads and power grids – takes on vital significance. S.M.A.R.T policing deals with various aspects of policing that are sustainable and holistic.

S	M	A	R	T	Policing
Sensitive and strict	Modern and mobile	Alert and accountable	Reliable and responsive	Techno-savvy and trained	

There is a huge and unknown attack surface on smart cities. With so much complexity and interdependency, it is difficult to know what and how everything is exposed. Therefore, simple problems could have a huge impact due to interdependency and chain reactions. The police needs to evolve continuously and learn from each attack on the smart city. The repository of information should be enriched with various incidences and should be progressive in nature. This chapter discusses in detail the initiatives to be taken by S.M.A.R.T. police.

4.1. Sensitive and strict

In a smart city, the police has to be sensitive to the society's needs and strict toward the procedures and rules made for a peaceful society. In India, the police needs to be more accepted by the general public rather than inducing fear among citizens. Smart police should understand the citizen perspective and partner with social organizations to provide a safer environment.

Partnership with society

Community policing has been around for some time in India, but is not effectively utilized by all departments in all areas. Partnership with society can be in various forms – rotary clubs, mothers against drunken driving, schools for inculcating traffic sense in children, residents to keep an eye on child kidnapping, businesses to help increase vigilance in market areas, etc. Partnering with society would improve the public image of police and would also provide eyes and ears to the police department.

Partnership between police and pawn shops

Chief Kim Jacobs of the Columbus, Ohio, police department partnered with pawn shops and scrap yards in the area. The goal was to reduce thefts by targeting burglars and thieves who are repeat offenders. The city compiled a computerized "do-not-buy" list of more than 22,000 individuals convicted of theft or a theft-related offense in Columbus or surrounding areas within the past six years. The city shared the electronic list quarterly with scrap yards and pawn shops, which were prohibited from purchasing goods from anyone on the list. Anyone caught purchasing goods from someone on the list could be charged with a misdemeanor and owners could lose their business license.

Understanding citizen perspective

All activities must be tested to ensure that they add value for the citizens. This is difficult to achieve in a policing scenario. In smart cities, police would have to address the convenience of the citizen and provide services within a defined turnaround. Smart police can run campaigns that encourage citizen participation, devise mechanisms for periodic feedback and processes to incorporate suggestions from the citizens.

4.2. Modern and mobile

In smart cities, governments want to deliver better infrastructure and services in all domains – education, health care, transport, energy, policing and others. Substantial funds are required to meet such expectations. The police service is a significant organization not only in terms of cost, but also in terms of its impact on society. The police service, therefore, needs to be modern and mobile to maintain public confidence and trust in the services it provides.

Social media

Police departments are using social media for two basic purposes: disseminating their own messages to the public, and gathering information from social media platforms to prevent and investigate crimes. Police can use social media to facilitate criminal investigations (e.g., observing suspects' postings on social media for self-incriminating comments), be aware of the mood of the public during major demonstrations, share important information with the public during times of crisis as well as about everyday news and events, receive crime tips, and receive crime reports.

Social media to track trending topics

The Los Angeles Police Department (LAPD) has used social media to help guide department operations during major events such as the NBA All Star Game in 2011 and the Stanley Cup playoffs in 2012. During these events, the department tracked large-scale parties and other gatherings throughout the city, and deployed teams of building inspectors, police officers, and fire department officials to ensure the events were legal and safe. The department also monitored social media to keep a tab on "trending" topics, such as whether large crowds of people planned to head downtown, and adjusted deployment plans accordingly. The LAPD has fully integrated its social media branch into the command post structure for major events. The social media branch is responsible for briefing the incident commander about relevant activities on social media.

Public safety broadband network

In the event of crisis, it becomes essential for police departments to interact with each other and coordinate their efforts to safeguard citizens. However, in a crisis, network bandwidth becomes unavailable. Police should be provided a secure, reliable and dedicated interoperable network for emergency responders to communicate during an emergency. Dedicated radio spectrum for emergency services should be allotted and maintained by the police departments.

Mobile technology

If officers have mobile devices – such as tablets or smartphones – they will be able to work more efficiently. Rather than filling in forms a number of times, officers could complete tasks once and submit information back to central systems remotely. They could also have access to more information while on patrol, enabling them to make better decisions. Multiple state police departments in India are investing in mobile technology for their patrolling vehicles. Mobile technology can be used by police command centers to deliver emergency calls to the patrol vehicle, to capture the images of incidents that can be used for investigation, to challan with real-time information of the vehicles, capture data quickly, and perform all the office functions from the patrol vehicle only.

Implementing mobile technology successfully in Leicestershire

The Loughborough University assisted the Leicestershire Police with procuring and implementing mobile devices in 2008. In particular, the force wanted to reduce its running costs. The university assessed the tasks that police officers needed to complete on a daily basis. It found that officers were going to a crime scene, filling in a report, coming back to the station, and faxing it to the Criminal Records Bureau, which would then upload it to a computer. The whole process took two to three days. The university considered how the force could implement mobile data terminals so officers could complete these tasks more efficiently. The force identified £5.2 million of efficiency savings from 2008 to 2011 as a direct result of the new mobile devices. In addition, police visibility increased by 44%, crime reduced by 26% and public confidence doubled to 85%.

Mobility

Police should be equipped with appropriate mobility means to respond to situations in any impacted area. Given the vertical expansion of smart cities and high density of population, police should be able to reach the incident location in minimum timeframe. This would mean better vehicles, aerial surveillance, drones, quad copters, automated vehicles etc. to be included in the police infrastructure as per requirement.

4.3. Alert and accountable

The key to alertness would be partnerships among police departments to increase coordination of their crime-fighting strategies. Partnerships can serve as an efficient, cost-saving way for departments to share the costs of certain functions, while combining the skills of multiple departments. It provides a pool of data that can be converted into meaningful information. The accountability of the police department also increases in a smart city. The police is accountable for various actions taken by them to secure the citizens.

Developing a performance culture

Smart policing requires a performance-tracking system that breaks down top-level objectives into clear, measurable targets that policemen at every level must understand, accept, and meet. When performance is not up to the standard, action is required. Tackling problems quickly and holding colleagues accountable for poor performance raises efficiency as well as morale. Every team member of the smart police should be encouraged to help the team when its performance dips. The culture change in the police organization would help them bond and serve the citizens as a collective body.

Partnership with other police departments

Partnership could be achieved at various levels, such as the sharing of data, applications, people, intelligence and resources. The most basic way of partnering with neighboring state police departments is to use compatible technologies to create an intelligence network. In India, the National Crime Record Bureau (NCRB) is mandated to collect and share data from police organizations. NCRB is also implementing Crime and Criminal Tracking Network and Systems (CCTNS), which is a mission mode project to track criminals through a single system. A single system will increase the alertness of police by providing track of crime and criminals in other States.

Partnership with universities and other researchers

Police departments have large volumes of information collected through various means. With the implementation of CCTNS, this information will be available in digital format as well. However, police departments are often unable to comprehend the information available in a useful manner.

Police departments can collaborate with universities, researchers and criminal justice students to help analyze data so that it may be more productively utilized. The effectiveness of programs and events launched by police departments can be studied by the students of universities. This gives good exposure to students in academic projects and provides useful insights to police departments about their programs. Another way of collaboration is through guest lectures by university professors to police officials. These lectures may focus on newer technologies or motivational aspects. Partnership with universities and researchers would benefit both the police department and the academia.

New organization structure for police departments

Multiple levels/ hierarchy in Police departments lead to slow processing and reduce innovation capacity. There are several advantages of flatter organization structures in police departments. First, flatter structures tend to experience fewer communications barriers. Second, they are better at spreading ideas. They also make it easier to establish clear lines of responsibility.

Given the widespread use of technology for information sharing and envisaged use of technology for core processes, the need for multiple levels would reduce in future, making the police officers more accountable. Police departments can look at hiring retired offers as domain specialists, given the depth of knowledge, years of experience and lower personnel cost of retired officers. New organization structures should be proposed for police departments to reduce the turnaround time of police processes.

Public private partnerships

The US, the UK and Australia have developed public-private partnerships in policing. These include both the police department's contracting out of policing functions to private agents, and the development of collaborations between sworn police and private security agents operating independently in a particular jurisdiction. Retired police officers can be hired as private agents to outsource activities such as fingerprinting, issuing of parking tickets, enforcing traffic violations, doing investigative follow-up work, and preparing affidavits for police. Back-office work of police agencies can also be outsourced to private agents.

Informal arrangements have been around for a while as community policing. More formalized methods for partnering with private security need to be devised to increase the strength of policing in the area. Public-private partnerships create rich opportunities for law enforcement agencies to leverage their scarce resources toward serving the public more effectively and efficiently. This arrangement increases the overall level of alertness in the society.

4.4. Reliable and responsive

The diversity of safety and security challenges faced by smart cities means the police force must plan holistic safeguarding measures. Solution providers are moving away from standalone products and systems toward networked solutions, which cover the entire security concept and are more reliable. The police force needs to become reliable and responsive to reduce crimes, improve confidence and support victims.

Multiple input mechanism for emergency response system

In smart cities, multiple input mechanisms should be available to connect with emergency response services of the police. The input mechanisms may range from phone calls, text messages, emails, voice over IP, messengers, IoT alarms, etc. Facilities to cater to differently abled people should be built in to the new emergency response system. Easy data transmission and critical information sharing can significantly enhance decision-making, and the response and quality of service provided to emergency callers. Messages, photographs and videos received by the emergency response system can be used later for judicial purposes and to create awareness among citizens.

Threat modelling

With the emergence of smart cities, decision makers in smart policing should not be limited to the awareness of the threat posed by the attackers, but also how to measure the consequences associated with the criminal activity. For example, drug trafficking poses financial, social and health threats to the society. Police should develop threat models to assess the overall size and cost of crime occurring in the city. Threat modelling can be done by identifying the threats and vulnerabilities in the first step, and then assessing risks associated with the threats. Threat modelling would enable risk assessment across diverse areas including immigration, customs, terrorism, biosecurity and emergency management. Despite some models being used around the world, detailed assessment frameworks and methodologies need to be developed by the police.

Threat modelling around the world

In the UK, the Serious Organised Crime Agency (SOCA) issues an annual Threat Assessment of Serious Organized Crime, which is based on strategic intelligence work and is aimed at estimating the harm to society by organized serious crimes.

In Canada, the Royal Canadian Mounted Police (RCMP) has developed Sleipnir, a framework that quantitatively measures the relative threat posed by different organized criminal groups. This model has been adopted and modified by other policing agencies in Australia and the UK.

4.5. Techno-savvy and trained

Intelligence-led policing is a concept that involves a number of factors coming together. It has been defined as "a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention." Techno-savvy and trained police targets prolific and serious criminal offenders in an organized, thoughtful manner. With the growing amount of data in smart cities, techno-savvy policing would gather a wide variety of data from various sources for analysis and required actions.

Defining and managing end-to-end process

Multiple departments are involved in the end-to-end judicial process – police, prisons, judiciary, special agencies, forensics, etc. These departments have separate processes, separate systems and multiple owners for the same process. Coordination failures are common, leading to delayed judgments, and high opportunity costs. To overcome such difficulties, decision makers should develop a shared understanding of the entire judicial process. Smart policing objectives would be achieved when the entire value chain works in tandem and uses interlinked technology systems to provide services to citizens.

Building capacity in the right skills

With the growing smart technologies, a basic level of IT knowledge should be mandated for new recruits of police departments. Basic IT skills would help them learn the technology faster and develop the skills easily. Police should define career paths in specialized skills such as forensics and cybercrime to support the growth of joining officers. Police departments should take the help of universities to identify in advance the new streams for skill development. A right mix of skills should be made part of smart police in each area.

Cybercrime management

Cybercrime is vastly under-reported, but even the crimes that are reported show that this problem is increasing rapidly. For example, a single cybercrime attack against banks in 2013 involved US$45 million in losses — more than the total losses from all "traditional" bank robberies in 2011. With the increasingly connected environment of smart cities, the problem of cybercrime would multiply manifold. Cybercrime can result in not only financial theft but also theft of personal information. All police officers should receive a certain degree of training about cybercrime, so that they are able to respond to victims in an intelligent way, know what questions to ask, and provide helpful information to residents about protecting themselves against scams and cybercriminals.

In addition, police departments should have a number of cybercrime experts who have received a much higher level of training. Policies and laws should be made to appropriately punish cyber criminals. Partnerships are critically important in the field of cybercrime. Task forces with other local, state, and central law enforcement agencies can lessen the burden on individual police departments. Universities can also be an excellent resource.

Effective use of data

With the growth of technology, police departments are generating large volumes of digitized data such as surveillance videos, digitized records of criminals, social media feeds, forensic reports, etc. These should improve decision-making by officers. However, identifying relevant information and analyzing vast amounts of data will require appropriate resources. Smart policing would have to invest in the right resources in terms of technology and manpower to analyze the data trends and take preventive measures to safeguard citizens.

05 Key recommendations

The "Policy Roundtable - SMART Policing" was conducted under the aegis of FICCI and the Indian Police Foundation - IPS (Central) Association in FICCI auditorium on 10 July 2015. The participants were a judicious mix of serving and retired senior officers involved in the law enforcement process, eminent personalities from civil society, senior functionaries from FICCI, renowned journalists and representatives from industries, both technology and advisory. The recommendations from the roundtable supporting S.M.A.R.T. policing are provided below.

5.1. Sensitive and strict

a. A multi-disciplinary approach to police reforms is needed, involving different stakeholders including civil society, industry, academia, lawyers, media, etc.

b. There is an urgent need to introduce Citizens' Charter in a time-bound fashion to ensure high standards of service delivery to citizens. The charter should envision the growth of smart cities and related technologies.

c. A concerted effort to improve the living and working conditions of policemen should be made to increase their commitment to their service.

5.2. Modern and mobile

a. Leading practices should be introduced through the optimal use of technology in a time-bound manner. This could be ensured by obtaining professional help and freeing core resources for policing work.

5.3. Alert and accountable

a. The need of the hour is systemic reforms that free the police force from illegitimate interferences and insulate it from external pressures. There is a need for long-term strategic planning to strengthen the policy framework in order to fully realize India's vision for homeland security and encourage greater public-private participation.

b. Forces need to be equipped with functional autonomy. The police should be free from extraneous influences and should be provided with functional and financial autonomy. At the same time, the police leadership should be held accountable for ensuring peace and satisfactory services to the people.

c. Promotion of good governance, accountability and transparency in policing should be encouraged. Measures are needed to ensure that police is made accountable. A commitment to the rule of law and a humane police force, one that is not dreaded by the people, is the need of the hour.

d. Public-private partnership and partnerships with technology and system integrators should be encouraged to introduce newer technologies in the police functioning from time to time.

5.4. Reliable and responsive

a. Increased use of technology in police work and creating Standard Operating Procedures (SOPs) for effective delivery of services

5.5. Techno-savvy and trained

a. Recruiting skilled manpower through a transparent recruitment process would enhance the image and reputation of policemen. This would increase productivity and support more activities with leaner organization.

b. Training would improve the skills and efficiency of policemen. World class training institutes for police recruits and in-service trainees should be established and maintained. Training should also compile best practices in community policing, deployment of technology, modernization of control rooms, evidence-based policy in policing, and standardization of police service delivery in the curriculum.

c. To address the security needs of the smart city, capacity should be built across various areas, such as:

- Training and infrastructure development to tackle new age crimes
- Build expertise and well-researched domain knowledge to deal with the challenges faced by the police and security establishment
- Build expertise to support policing and Intelligence Services – cryptologists, analysts, language experts, forensic experts, etc.
- Think tank on policing could be brought together as experts to encourage research on specific aspects of policing, to build domain knowledge, test and validate existing practices and to standardize teaching, police training and police practice
- Set up central repository of knowledge on important areas concerning policing
- Capacity-building outreach and collaboration for effective crime prevention interventions

d. Leveraging IT, including the use of mobile technologies and social media, should be encouraged

e. Use of technology to deal with the issues of cybercrime, cybersecurity, data privacy and other areas linked to the use of the internet and availability of data on the internet

f. Creating centralized and connected databases of crime, criminal records, people verification, historic analysis of place of incident, etc. that would help in establishing linkages among people and places

6. References

a. Police Executive Research Forum. 2014. Future Trends in Policing. Washington, D.C.: Office of Community Oriented Policing Services.

b. Smart policing: how the Metropolitan Police Service can make better use of technology, Greater London Authority, August 2013.

c. Patrick F. Walsh, Intelligence and Intelligence Analysis (Routledge, 2011)

d. 'Meaningful adjacencies': How the names on the 9/11 Memorial were arranged, The Week, 8 September 2011.

e. Data Breach Investigations report, 2015

f. Beniamino Murgante and Giuseppe Borruso, Cities and Smartness: A Critical Analysis of Opportunities and Risk, 2013

g. Cities at risk: 5 that were victims of cyberattacks, Smart Cities Council, 24 July 2015.

h. Data on Police Organizations in India, Bureau of Police Research and Development, 2014

i. Public private partnerships in policing, What-when-how. com

j. Dr. Sally Leivesley, Smart cities

k. Harry Barton, Lean policing: Initial findings from a study of 5 UK police forces, 2013

l. Adel S. Elmaghraby, Michael M. Losavio, Cyber security challenges in Smart Cities: Safety, security and privacy, Journal of Advanced Research, July 2014

FICCI contacts

Sumeet Gupta
Director
sumeet.gupta@ficci.com

Gaurav Gaur
Assistant Director
gaurav.gaur@ficci.com

FICCI, Federation House, Tansen Marg,
New Delhi 110 001
Tel: +91-11- 23487237 (D) +91-11-2373 8760-70 (Ext. 237)
Fax: +91-11-23765333

EY contacts

Rahul Rishi
Partner
+91 116 623 3183
Rahul.Rishi@in.ey.com

Akshya Singhal
Director
+91 11 66233277
Akshya.Singhal@in.ey.com

Mala Gautam
Manager
+91 124 6711379
Mala.Gautam@in.ey.com

Our offices

Ahmedabad
2nd floor, Shivalik Ishaan
Near C.N. Vidhyalaya
Ambawadi
Ahmedabad - 380 015
Tel: + 91 79 6608 3800
Fax: + 91 79 6608 3900

Bengaluru
12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 4027 5000
+ 91 80 6727 5000
Fax: + 91 80 2210 6000 (12th floor)
Fax: + 91 80 2224 0695 (13th floor)

1st Floor, Prestige Emerald
No. 4, Madras Bank Road
Lavelle Road Junction
Bengaluru - 560 001
Tel: + 91 80 6727 5000
Fax: + 91 80 2222 4112

Chandigarh
1st Floor, SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh - 160 009
Tel: + 91 172 671 7800
Fax: + 91 172 671 7888

Chennai
Tidel Park, 6th & 7th Floor
A Block (Module 601,701-702)
No.4, Rajiv Gandhi Salai, Taramani
Chennai - 600113
Tel: + 91 44 6654 8100
Fax: + 91 44 2254 0120

Hyderabad
Oval Office, 18, iLabs Centre
Hitech City, Madhapur
Hyderabad - 500081
Tel: + 91 40 6736 2000
Fax: + 91 40 6736 2200

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682304
Tel: + 91 484 304 4000
Fax: + 91 484 270 5393

Kolkata
22 Camac Street
3rd floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400
Fax: + 91 33 2281 7750

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400028
Tel: + 91 022 6192 0000
Fax: + 91 022 6192 1000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 3000

NCR
Golf View Corporate Tower B
Near DLF Golf Course
Sector 42
Gurgaon - 122002
Tel: + 91 124 464 4000
Fax: + 91 124 464 4050

6th floor, HT House
18-20 Kasturba Gandhi Marg
New Delhi - 110 001
Tel: + 91 11 4363 3000
Fax: + 91 11 4363 3200

4th & 5th Floor, Plot No 2B, Tower 2, Sector 126,
NOIDA 201 304
Gautam Budh Nagar, U.P. India
Tel: + 91 120 671 7000
Fax: + 91 120 671 7171

Pune
C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 6603 6000
Fax: + 91 20 6601 5900

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN1508-094
ED 0516

JS

EY refers to the global organization, and/or one or more of the independent member firms of Ernst & Young Global Limited

About FICCI

Established in 1927, FICCI is the largest and oldest apex business organisation in India. Its history is closely interwoven with India's struggle for independence, its industrialization, and its emergence as one of the most rapidly growing global economies.

A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate, engaging with policy makers and civil society, FICCI articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies.

FICCI provides a platform for networking and consensus building within and across sectors and is the first port of call for Indian industry, policy makers and the international business community.