MISTRAL
...Partners in Real Time

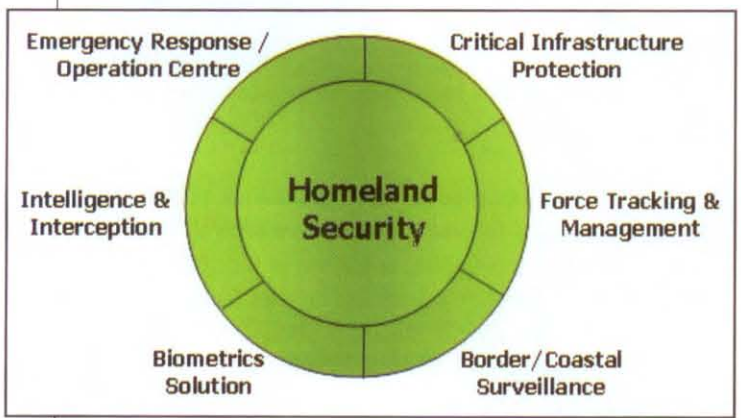
Integrated C4ISR for Homeland Security

By **Anees Ahmed** – Chairman & Co-Founder, Mistral Solutions Pvt. Ltd.

Introduction

Security is critical, be it against terror attacks, pilferage of national resources or even domestic riots with damage to critical local infrastructure. Citizen and infrastructure protection is the most important security aspect for a country. In our country this factor is further emphasized, given the increasing prominence for brand India in the global arena. India is also playing host to international events involving visiting government dignitaries and prominent international personalities; it is equally important that security systems be deployed effectively and efficiently allowing these events to proceed smoothly.

India is projected to emerge as one of the largest players in the global homeland security market by 2020. The Ministry of Home Affairs announced plans to create a National Information Grid that can essentially integrate the existing databases of intelligence and enforcement agencies across the country. The Government of India has also expedited the acquisition of critical equipment and items to improve the homeland security infrastructure.



With the increasing frequency and diverse nature of threats to the country, what previously used to take place as uncoordinated activities by different branches and chapters of law-enforcement agencies, is now consolidated under an architecture that allows disparate agencies and their chapters to gather specific and useful information, and share the same across a network of interested parties. This architecture, loosely termed homeland security is today seen as vital to the continued survival of the state. Homeland security needs to leverage the technological advances and practices of the day and keep pace with the increasing technological prowess of sources of threats.

The penetration of technology is high and complex in the homeland security domain, given that there are different areas to be considered such as baggage screening, biometric passports, video surveillance, public safety networks, wireless broadband systems, radar systems and cyberspace surveillance, among others. Broadly, homeland security encompasses border and coastal surveillance, force tracking and management, critical infrastructure protection, emergency response/operation center, mobile command and control, intelligence and interception, and biometrics solution.

C4ISR – are they really integrated?

C4ISR, adapted from its military origins, is a framework for organizing the variety of information emanating from a situation (typically a crisis) in a manner that enables non-local users to analyse such information (from multiple sources); act on that information or advise local players on actions to be taken; receive feedback from local players on actions taken, based on which a follow-up set of actions or advice can be

initiated towards the objective of resolving the situation to the advantage of the users. C4ISR systems make extensive use of technology.

Effective C4ISR components

Stakeholders

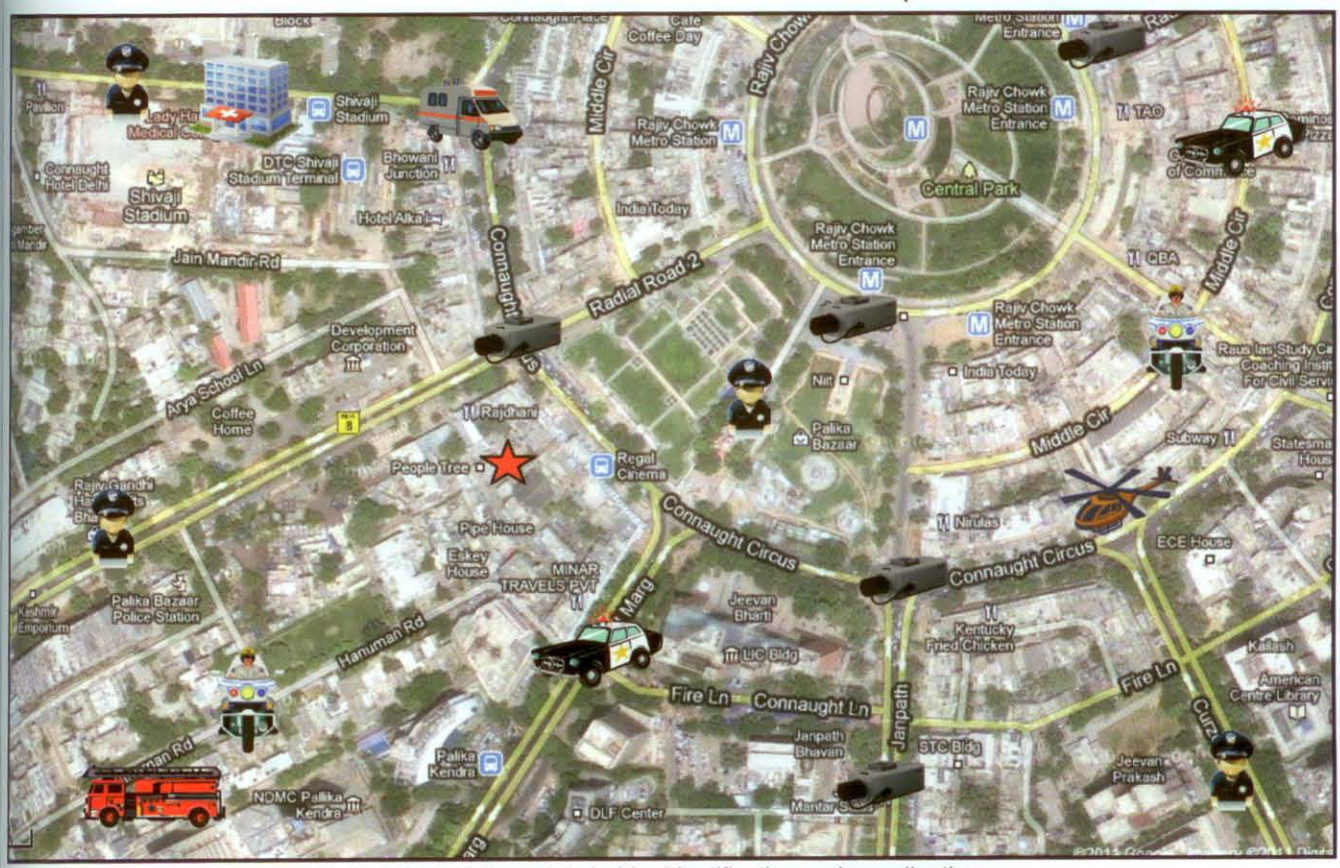
For a C4ISR system to be effective, involving all stakeholder groups for providing solutions to any emergency or accident scene is critical. Imagine an emergency situation similar to the December 2004 tsunami that hit the south-eastern coast of India. The power department representatives, water/sanitation department, local hospitals and police force had to be involved on an immediate basis, followed by Air Force personnel to air-lift trapped civilians, and maybe even the Armed Forces to avoid crimes being committed in the ensuing chaos. For quick action and assistance to the local people, it would be essential for all the departments to be connected through a single communication system that can be centrally monitored by personnel based in the headquarters. This would ensure quick and simultaneous transfer of information, including video, images and data, which can help the authorities take quick decision and alert the on-field staff simultaneously.

A comprehensive and all-encompassing security system should involve different stakeholder bodies such as the Coast Guard, Navy, Army, paramilitary forces, airport authorities, metros, ports, critical sites, border security personnel, fire services, intelligence, EOC/EMC, rescue operations representatives and medical response units working seamlessly as a single cohesive unit.

Sensors

Sensors are the eyes, ears and skin of a surveillance network, and the effectiveness of the surveillance set-up in a particular environment is critically dependent on the type and specifications of the sensors employed in the network. For example, what use is a surveillance camera without IR-illuminators for a 24x7 surveillance operation? If the camera does not provide a WDR (Wide Dynamic Range) feature or include the ambient light sensitivity and compensation, the security system will neither be comprehensive nor meet the requirements of the security operation.

There is a variety of sensor technologies in the market such as wired and wireless IP video, megapixel cameras, IR



Situation clarity – stakeholder identification and coordination

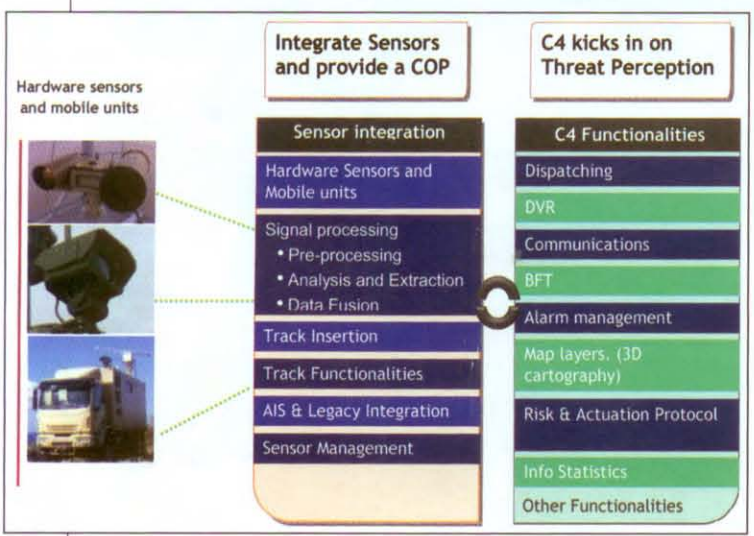
Combination of sensors on a surveillance network

cameras, thermal cameras, access control, induction loop sensors, video wall, video analytics, fire detectors, movement detectors, vibration detectors, IR barrier, RF barrier, etc. Each of these sensors provides unique data/ images that can be combined in different ways to get a comprehensive image/ data source of the situation or area being surveyed.

Choosing a sensor technology will be a function of parameters such as cost (or budget), the potential entities-under-surveillance, surveillance range, the terrain of the area-under-surveillance, and the features to be captured (of the entities-under-surveillance).

Open system structure

Sensor-independence allows the solution to integrate new sensors (based on new technologies) at a future point in time. Cartographic independence allows the solution to support a variety of map formats. A decentralized and Services-Oriented-Architecture (SOA) allows the system to be managed from any fixed or mobile network device, providing an added robustness in the event of failures or crisis situations.



Open System Structure

In an open system, an integrated management console can be set up that will allow the users to monitor many types of sub-systems such as call processing, sensors, DVR/ NVR, computer-aided dispatching, AVL, interactive voice response, data management, GIS and emergency notification, amongst others. The user would have to dispatch information to the first line of emergency responders, share video streams in real-time for remote or local monitoring and review/ analysis, Blue Force Tracking (BFT) for quick on-field response and simultaneously do other functionalities related to the event.

Vendor agnostic platforms

Integration of old and new technologies is essential in our country. To start with, it need not be mandatory for all security and law enforcement agencies to upgrade their old technology-based communications equipment in order to set up the latest network. C4ISR solutions have to be vendor agnostic platforms that can link any type of communications technology or brand with others. These communications technologies could include some or all of the following – PABX or GSM/ GPRS telephone lines, PMR or UHF/VHF/HF radio, trunking (Analogue-MPT1327, TETRA-P25, TETRAPOL), VoIP (VoIP-SIP/H323, Gateways), or others such as PA systems and intercoms. Not just communications equipment, the integration also has to happen with different types and brands of sensors into the system, including both old and new technologies.

Key elements for success

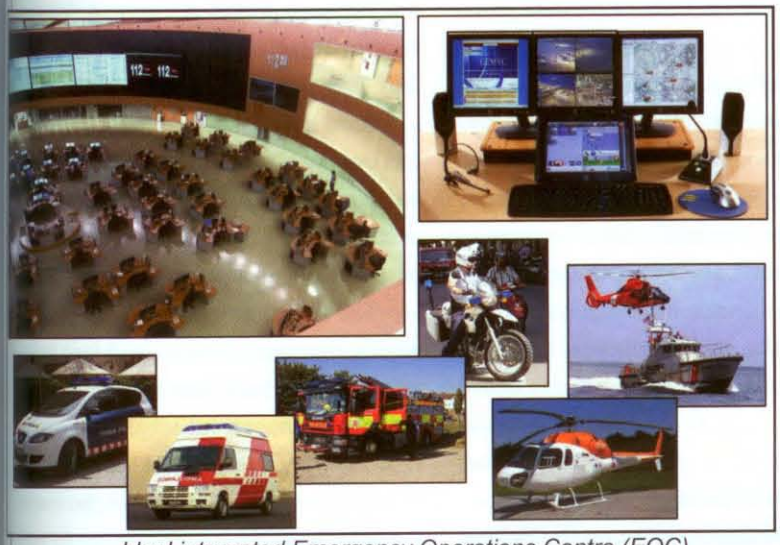
Integration with legacy systems

Seamless integration of the different components of a security system is essential to obtain maximum efficiency and effectiveness. The integration also needs to extend to backend applications such as e-governance systems and other online and IT systems. While existing systems have to be re-used, the technology and equipment used in the systems have to be upgraded continuously to keep abreast with technology developments globally.

Ease of use

For field staff who deal with a multitude of incidents and people, the systems and the user interfaces have to be

simple and uncomplicated. Hi-tech gadgets and software that require intensive training will not serve the purpose. If the man on the ground cannot use it, it is useless! Any type of complexity will mean that the system will not be used. Complexities and advanced technologies have to be hidden at the back-end of the system. It is essential to remember that while the design of these security systems is being done by engineers, the end-user of the system is not an engineer. The system has to be capable of providing data from any database and at any time.



Ideal integrated Emergency Operations Centre (EOC)

Integrated C4ISR solutions from Mistral

Mistral's Homeland Security business group offers ready-to-deploy, proven, high-technology solutions for strategic and tactical requirements. The technologies available from Mistral are ideal to build effective, efficient and essential solutions. These solutions include various types and makes of edge-devices and applications that address the systemic needs of homeland security planners. The various system integration solutions from Mistral are based on the C4ISR concept. In addition, Mistral's expertise as an engineering house helps provide customers with customized solutions from concept to deployment.

The Mobile C4ISR Platforms from Mistral are a range of unique vehicles that are easily deployable solutions for tactical operations and other security requirements. The solution consists of a customized vehicle with either or all of the following: IP video surveillance equipment, command and control module, video management, and analytics and monitoring stations.

The video surveillance solution consisting of wireless/ wired fixed IP cameras, wired IP PTZ cameras, network video recorder and video management software (VMS) offers long-range wired and wireless capability coupled with high-quality video and audio, with on-site and remote video management. The command and control modules provide a group of functions for integrated emergency management; the three modules under this include call-taking and dispatch, communications matrix, and cartography mapping and resource locator.

Mistral provides solutions for 'Dial 100,' Safe City, mass transit security, critical infrastructure protection, mobile command and control, and other critical security applications.

Communications: Ability to integrate various communication protocols: GSM, VHF/UHF/HF, Tetra, PSN, etc.
Computing: Applications such as Cartography, Databases, Simulation, Analytics; and functionality such as interoperability of systems, handling multi-media content
Command: Tools for Data Mining, Decision Support System (DSS), etc.
Control: Real-time transmission and receipt of all information, under any circumstance, using protocols
Intelligence: Human Intelligence, Signal Intelligence
Surveillance: Sensors
Reconnaissance: Sensors, Sensor carrier

C4ISR Components

Conclusion

The security of a country is largely dependent on a number of groups of people working in tandem through the use of a variety of technology-led systems and components. While the focus on homeland security in India has only recently increased manifold, it will take a long time for the systems to be established and function efficiently. The current technology needs of the Indian homeland security industry have to be systematically and strategically met that will ensure that the future is secure for the next generation. ■

- All illustrations in this article are the property of the author.