₹ 100 US$ 10

GEO intelligence

VOL. 1 ISSUE. 1 Jan - FEB 2011

GeoPDF

Geospatial intelligence for warfighter P.24

Data sharing

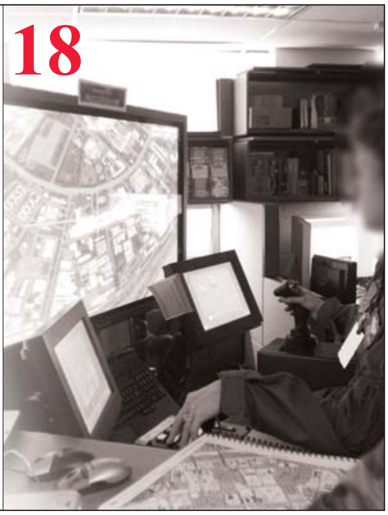
Challenges for intelligence community P.28

C4ISR

Harnessing tech for optimum security

P.18

GIS DEVELOPMENT PUBLICATION



ARTICLES

Geo Intelligence

Chairman MP Narayanan
Publisher Sanjay Kumar

Publication Team
Director Publications Niraj
Associate Editor Bhanu Rekha
Assistant Editor Deepali Roy, Aditi Bhan
Sub-Editor Anand Kashyap

Designed by Deepak Kumar
Manoj Kumar Singh

Circulation Team
Circulation Manager Priyanka Ujwal,
Vijay Kumar Singh

Owner, Publisher & Printer Sanjay Kumar
Printed at M. P. Printers, B - 220, Phase-II,
Noida - 201 301, Gautam Budh Nagar (UP)
India Publication Address A - 92, Sector - 52,
Gautam Budh Nagar, Noida, India **Editor**
Sanjay Kumar

Price ₹ 100, US$ 10

GIS Development Pvt Ltd
A-145, Sector 63, Noida, India
Tel +91 120 4612500 Fax +91 120
4612555/666

GIS Development does not necessarily subscribe to the views expressed in the publication. All views expressed in this issue are those of the contributors. The publication is not responsible for any loss to anyone due to the information provided.

PREVIEW

EVENT REPORTS

SECTIONS

Cover image courtesy
www.integrator.hanscom.af.mil

Harnessing tech for optimum security

Homeland security needs to keep pace with the increasing technological prowess of sources of threats. The adoption of Command, Control, Communications, Computing and Intelligence, Security, Reconnaissance (C4ISR), which makes extensive use of geospatial technologies, provides security forces the wherewithal to do so.

Anees Ahmed
CEO and Co-founder
Mistral Solutions

With the increasing frequency and diverse nature of threats to the State, 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, to keep pace with the increasing technological prowess of sources of threats. The adoption of C4ISR (Command, Control, Communications, Computing, and Intelligence, Security, Reconnaissance) concept, from military practice, provides homeland security the wherewithal to do so.

C4ISR can be thought of as a framework for organising multi-media information emanating from a situation (typically a crisis), in a manner that enables non-local users to analyse such information (from multiple sources); act

Border/Coastal Surveillance

Unregulated borders and coastlines are the chinks in a nation's homeland security armour. Smuggling (contraband and human trafficking), illegal immigration, and terrorism are the three threats to a country's security, most likely to exploit the porosity of unregulated borders and coastlines. Think of the 26 November Mumbai attacks or think of the smuggling of contraband through the borders of Gujarat, Jammu & Kashmir or Rajasthan. C4ISR Border/Coastal Surveillance Systems (B/CSS) seek to significantly reduce, if not eliminate, the incidence of such activities.

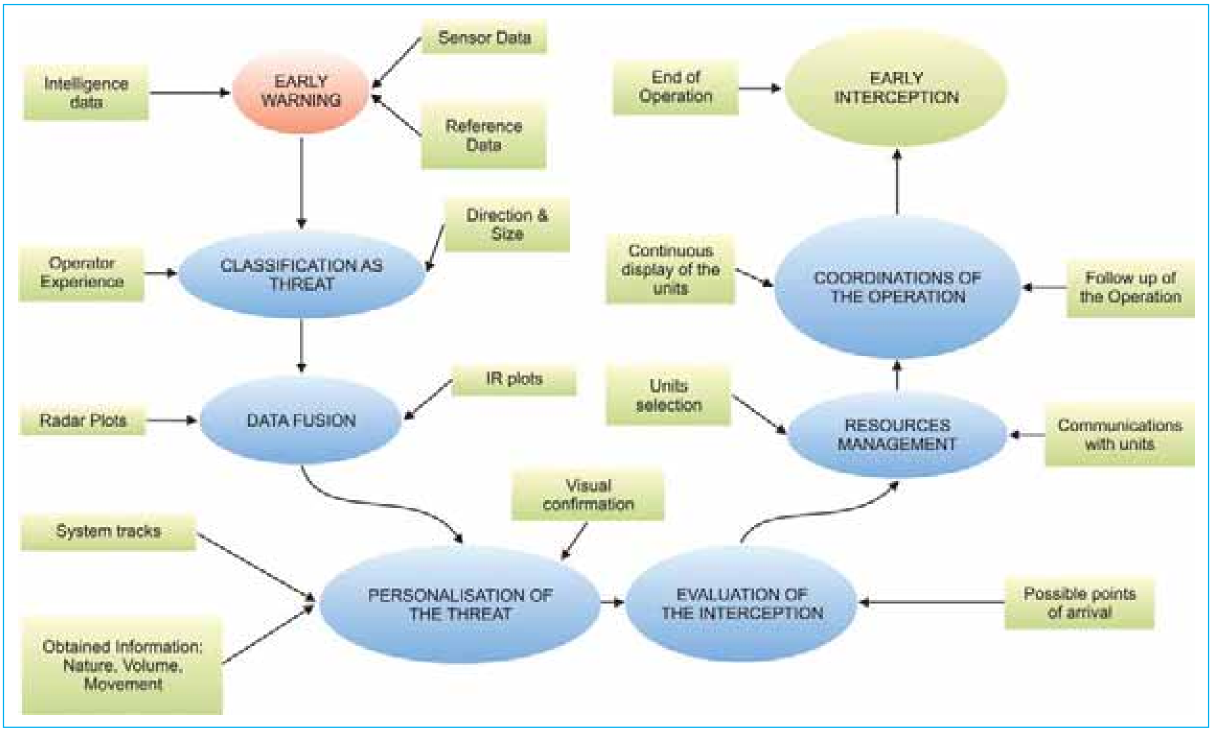


Figure 1: Operational components of a C4ISR solution

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, to resolve the situation to the advantage of the users. C4ISR systems make extensive use of technology: especially geospatial technologies.

Operational Components

Before going into further details of the technologies used in C4ISR solutions, it would be useful to gain a perspective on the operational components of a C4ISR solution, as applied to border/coastal surveillance (B/CSS) and critical infrastructure protection (CIP).

As can be seen from the above functional flow (Figure 1), there are four components of a C4ISR solution:

- Sensors (Remote Sensing)
- GPS
- GIS
- Command & Control Application

Sensors

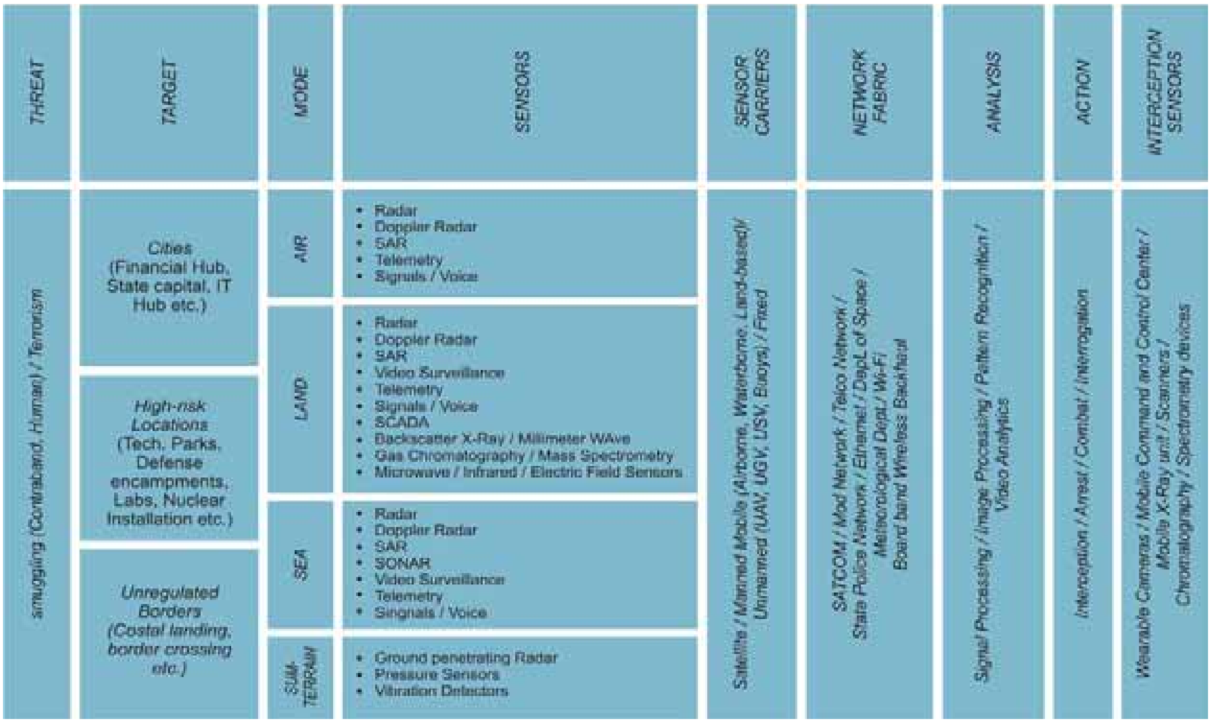
Sensors are the eyes, ears, and skin of a surveillance network, and the effectiveness of the surveillance set-up in a particular environment is critically dependent on the type and specifications of the sensors employed in the network.

How many times have we heard of a jewelry store heist where the surveillance footage was of little use because the resolution of the installed surveillance cameras was too low; because the lens used was not right; because the entrance-facing camera did not feature a WDR (Wide Dynamic Range) sensor or support BLC (back-light compensation).

There are a variety of sensor technologies in the market. Fig. 2 lists many of the popular sensor technologies, their delivery platforms, and the communications fabric, with respect to B/CSS and CIP requirements.

Critical Infrastructure Protection

Critical Infrastructure Protection (CIP) is the term used to refer to the systems and processes implemented to ensure that designated critical assets are protected from actions intended to curtail, seriously disrupt, or altogether prevent their functioning. A critical infrastructure need not refer only to physical assets of national importance (ports/airports, nuclear facilities, Parliament etc.); it may refer to any asset (physical, virtual) considered by an organisation (government, parastatal or private), as vital to its functioning. A C4ISR CIP solution provides comprehensive cover to key infrastructure.



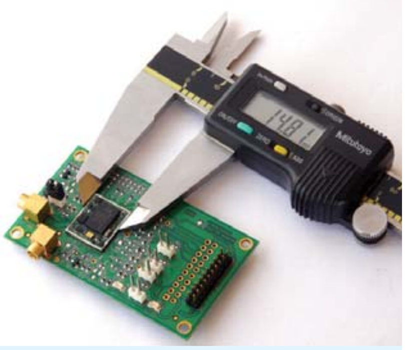
THREAT	TARGET	MODE	SENSORS	SENSOR CARRIERS	NETWORK FABRIC	ANALYSIS	ACTION	INTERCEPTION SENSORS
smuggling (Contraband, Human) / Terrorism	Cities (Financial Hub, State capital, IT Hub etc.)	AIR	• Radar • Doppler Radar • SAR • Telemetry • Signals / Voice	Satellite / Manned Mobile (Airborne, Waterborne, Land-based)/ Unmanned (UAV, UGV, USV, Buoys) / Fixed	SATCOM / Mod Network / Telco Network / State Police Network / Ethernet / DapL of Space / Meteorological Dept / Wi-Fi / Board band Wireless Backhaul	Signal Processing / Image Processing / Pattern Recognition / Video Analytics	Interception / Arrest / Combat / Interrogation	Wearable Cameras / Mobile Command and Control Center / Mobile X-Ray unit / Scanners / Chromatography / Spectrometry devices
	High-risk Locations (Tech. Parks, Defense encampments, Labs, Nuclear Installation etc.)	LAND	• Radar • Doppler Radar • SAR • Video Surveillance • Telemetry • Signals / Voice • SCADA • Backscatter X-Ray / Millimeter WAve • Gas Chromatography / Mass Spectrometry • Microwave / Infrared / Electric Field Sensors					
	Unregulated Borders (Costal landing, border crossing etc.)	SEA	• Radar • Doppler Radar • SAR • SONAR • Video Surveillance • Telemetry • Singnals / Voice					
		SUB-TERRAIN	• Ground penetrating Radar • Pressure Sensors • Vibration Detectors					

Figure 2: Sensor technologies and delivery platforms

Given a plethora of options, users typically apply the following thumb-rules when choosing among sensor technologies for specific situations:

- Implement a design comprising layers of sensors, with each layer delivering an increasing resolution of the entity-under-surveillance, as it approaches a defined boundary: for example, radars may be employed to track entities at a distance of 5-50 kilometres; long-range thermal cameras may be employed to track entities at a distance of 1-5 kilometres; and high-resolution optical cameras may be employed to track entities at a distance of one kilometer and below.
- Each layer may be a mix of technologies, such that blind-spots in one technology are visible in another; and such that counter-measures by the entity-under-surveillance do not render the entire surveillance layer dysfunctional: for example, in the case of surveillance on land, a mix of radars and vibration sensors may be implemented in one layer to preclude the possibility of the entity-under-surveillance evading observation by employing radar-masking techniques.
- Data from different sensor technologies can be combined to deliver a level of information significantly greater than can be provided by each of the individual technologies

GPS Receiver Module



Built around the SiRf Star III chip, the GPS Receiver Module from Mistral is the world's smallest high-sensitivity GPS module. The 20-channel GPS receiver is capable of giving accurate details of location, altitude, velocity, and direction. This fully functional RF module receives spread spectrum signals from the MEO (Medium Earth Orbiting) satellites.

It features a low-noise RF amplifier with sensitivity below -159dBm; and has the ability to withstand ESD up to 2000V. The GPS module is PCB mountable, with a very small footprint; and can be easily integrated in a wide range of applications in the defense and consumer electronics segment. These include portable navigation, cellular phones and other communication equipment.

in isolation. This data fusion is typically handled at the application level (command and control application or sensor management software).

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). Fig. 3 shows a range of sensors used in a typical CIP implementation.

GPS

The second important geospatial component of a C4ISR solution is the device that allows user resources to be tracked in real-time, in terms of location and movement. All C4ISR solutions include a Blue Force Tracking (BFT) module.

Blue Force Tracking (BFT) is a United States military term used to denote a GPS-enabled system that provides military commanders and forces with location information about friendly (and despite its name, also about hostile) military forces. In military symbology, the colour blue is typically used to designate friendly forces while red is used for enemies, and green or yellow are used for neutral forces.

A BFT system, at its simplest, consists of a GPS device and a means for relaying the GPS information to a monitoring centre: a police patrol unit may have a VHF radio set with the GPS device integrated in the microphone, so that location information is transmitted to the monitoring centre at the touch of a button. More sophisticated BFT systems will allow relaying of mobile sensor data, providing additional information specific to the location, etc.; along with the transmission of the coordinates.

Depending on the terrain being traversed, the GPS device will need to support a level of sensitivity that will allow it to function at all times.

GIS

The cartographic module is an important component of a C4ISR solution. A detailed digital representation of the area-under-surveillance will allow the user to integrate the data from the sensors and the GPS receivers on to map, and allow the user to associate real-time sensor feed with a location or feature on the map, as well as track its resources visually. The cartographic module typically imports maps from a third-party and then allows situation-specific interpretation to be imported or added to the maps. Multiple maps can be imported and used, provided they conform to widely used formats.

Command & Control Application

The command and control component integrates the feed from the sensors and GPS receivers with the cartographic representation of the area-under-surveillance, and allows the user to initiate SOPs in the event of an incident, query and receive additional information from sensors and resources in the field in real-time, and send out instructions to the resources on how to respond to an incident.

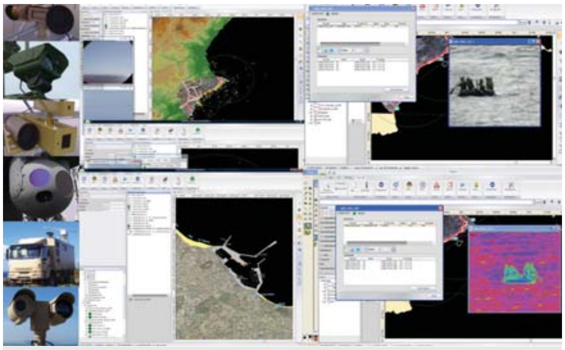


Figure 3: A mix of sensors in a C4ISR solution

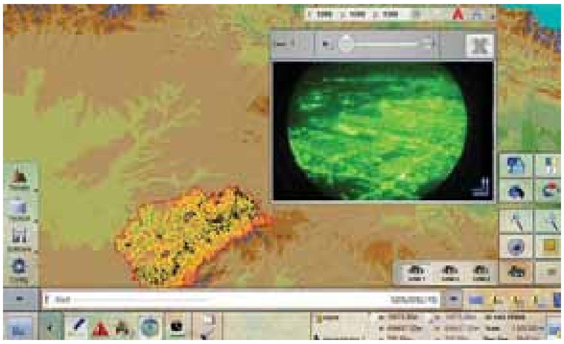


Figure 4: Cartographic representation with sensor feed

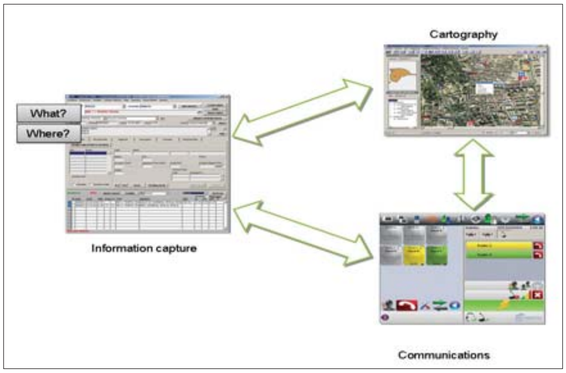
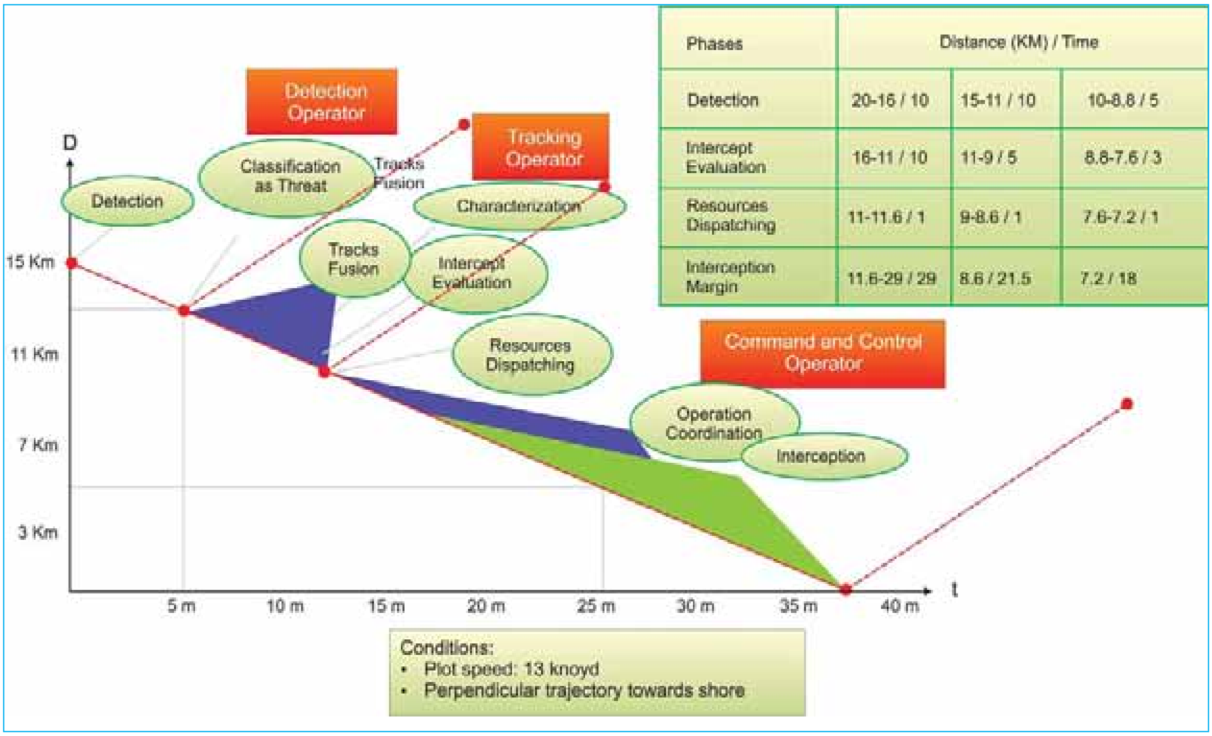


Figure 5: Integration of various components of a C4ISR solution

All this happens in a coordinated manner – even if there are multiple decision-makers participating from different locations – and with all available information at the fingertips of the decision-makers (common operational picture or COP). The command and control application sometimes also provides, through additional hardware, the capability to patch multiple communications protocols; thereby allowing different field units (some on V/U/



Phases	Distance (KM) / Time		
Detection	20-16 / 10	15-11 / 10	10-8.8 / 5
Intercept Evaluation	16-11 / 10	11-9 / 5	8.8-7.6 / 3
Resources Dispatching	11-11.6 / 1	9-8.6 / 1	7.6-7.2 / 1
Interception Margin	11.6-29 / 29	8.6 / 21.5	7.2 / 18

Conditions:
- Plot speed: 13 knoyd
- Perpendicular trajectory towards shore

Figure 6: Coastal surveillance system: Spanish case study – typical operational performance

HF, others on GSM or CDMA etc.) to communicate transparently with each other. Such a communications matrix is extremely effective in maintaining command and control during crisis situations.

Finally, given that duplication of information is bound to happen during an incident, the application automatically recognises the reports of an incident that are similar, and allows a user to de-duplicate such information.

Desiderata of a C4ISR homeland security solution

Choosing a Homeland Security solution – B/CSS or CIP – based on a C4ISR framework should be a decision taken on the basis of support for the following functionality:

Interoperability

By interacting with legacy systems of involved agencies and with deployed mobile units as well, it is possible to develop a higher resolution picture of a crisis situation. For this purpose, a data model such as the standard JC3IEDM should be used, and web services should be XML-based.

Sharing Mechanism

Sensor data should be managed by publication/subscription mechanisms: the operator subscribes to the information or services offered by the solution, which incorporates a middleware layer in charge of searching for the information and publishing it to subscribers. This allows information to be received and consolidated in a database in real time.

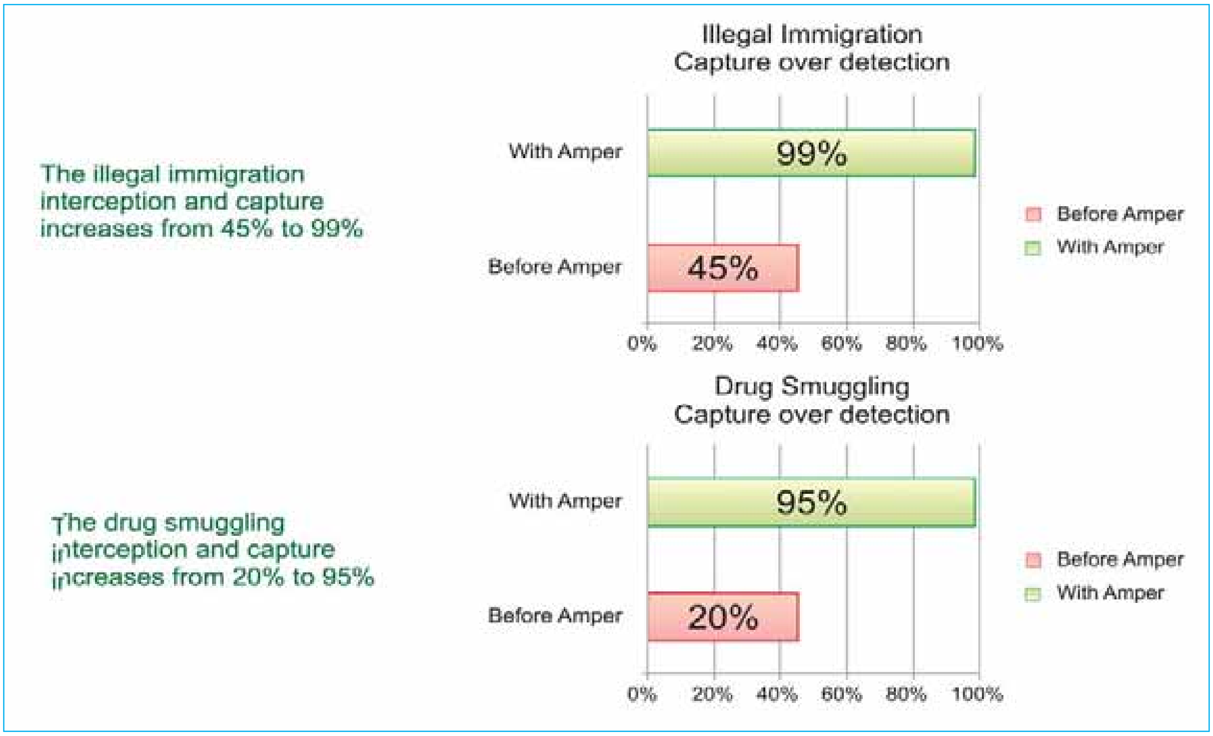
Openness

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.

Architecture

A decentralised and service-oriented-architecture (SOA)

> Given that duplication of information is bound to happen during an incident, the application automatically recognises the reports that are similar, and allows a user to de-duplicate such information



The illegal immigration interception and capture increases from 45% to 99%

The drug smuggling interception and capture increases from 20% to 95%

Figure 7: Coastal surveillance system: Spanish case study – operational impact

allows the system to be managed from any fixed or mobile network device, providing an added robustness, in the event of failure or crisis situation.

Low-bandwidth protocol:

Data synchronisation mechanisms used should allow information to be shared in real-time, at rates as low as less than 10 kbps, for the solution to function effectively in crisis situation.

Case Study

This case study is of a C4ISR B/CSS implementation in Spain, covering Spain's maritime border with North Africa (specifically Morocco). The problem Spanish authorities had was that this stretch of the maritime border was being used for illegal immigration and drug smuggling, and that the number of incidents were increasing at an alarming rate.

As can be seen in Fig. 6, the implemented system manages all phases involved in border management. The graph on the right plots the progress of the entity-under-surveillance towards the Spanish shore, with distance from the shore being plotted on the Y-axis, and elapsed time since detection being plotted on the X-axis.

The table on the right provides the phase-wise figures for three scenarios – detection at 20 to 16 kilometres, 15 to 11 kilometres, and 10 to 8 kilometres. The effect of the C4ISR B/CSS implementation, in this case, has been a staggering fall in the number of incidents featuring illegal crossing and drug-running across the maritime border covered by the solution.

Conclusion

Geospatial technologies can be used to deliver a far stronger implementation of homeland security solutions. In this connection, it is important to leverage the latest in the respective technologies (remote sensing, GPS, GIS) so that as detailed a COP (common operational picture) as possible is provided to decision-makers. In addition, these implementations, across various law-enforcement agencies, should support a level of interoperability that will allow them to share relevant information in real-time.

Homeland security is too critical a responsibility to be left to be addressed through silo-type responses. C4ISR solutions, leveraging the latest in geospatial technologies, promise and deliver significant improvements in the manner the State responds to threats to its existence.

All illustrations in this article are the property of Amper Sistemas and /or Mistral Solutions Pvt. Ltd. They cannot be copied and reproduced without the permission of the concerned parties