SP'S

AN SP GUIDE PUBLICATION

Special

SUPPLEMENT

TO C4I2 SUMMIT 2009

45 1964-2009 SP GUIDE PUBLICATIONS WIDENING HORIZONS...

SP GUIDE PUBLICATIONS Presents

C4I2 SUMMIT

ENHANCING INDIAN DEFENCE CAPABILITIES

In association with CNBC TV18 Profit From It.

THIS IS THE COMPUTER that alerted the aircraft about the tank crew trapped next to the target in an FM dead zone.

Mission-critical situations demand ultra-rugged, battle-tested computers. The DRS Military Rugged Tablet (MRT) delivers that and more. The MRT has a proven track record for withstanding the harshest conditions – 1,114 days in the field and counting. With the flexibility to be hard-mounted or dismounted, it's joint-ready whenever you are. No wonder it's already the rugged computing tablet of choice by 9 programs and counting in the Army, Air Force and Marine Corps.

For more information, visit **JointForceSystems.com**.

DRS TECHNOLOGIES

A Finmeccanica Company

Content

SP'S Special SUPPLEMENT TO C4I2 SUMMIT 2009
AN SP GUIDE PUBLICATION

PUBLISHER AND EDITOR-IN-CHIEF
Jayant Baranwal

SENIOR MANAGING EDITOR
Air Marshal (Retd) V.K. Bhatia

ASSISTANT EDITOR
Arundhati Das

SENIOR TECHNICAL GROUP EDITORS
Lt General (Retd) Naresh Chand
Lt General (Retd) V.K. Kapoor
Rear Admiral (Retd) S.K. Ramsay

CHIEF SPECIAL CORRESPONDENT
Sangeeta Saxena

CONTRIBUTORS
Lt General (Retd) S.R.R. Aiyengar
Air Marshal (Retd) A.K. Trikha
Brigadier Vinod Anand
Captain (Retd) T.N. Pranesha
Commander Devbrat Chakraborty
Anil Singhal

CHAIRMAN & MANAGING DIRECTOR
Jayant Baranwal

ADMIN & COORDINATION
Bharti Sharma

DESIGN & LAYOUT
ASSOCIATE ART DIRECTOR: Ratan Sonal
LAYOUT DESIGNERS: Raj Kumar Sharma, Vimlesh Kumar Yadav

SALES & MARKETING
DIRECTOR SALES & MARKETING: Neetu Dhulia
HEAD VERTICAL SALES: Rajeev Chugh
SALES MANAGER: Rajiv Ranjan

FOR ADVERTISING DETAILS CONTACT:
guidepub@vsnl.com
neetu@spguidepublications.com
rajeev.chugh@spguidepublications.com
r.ranjan@spguidepublications.com

SP GUIDE PUBLICATIONS PVT LTD
A-133 Arjun Nagar (Opposite Defence Colony),
New Delhi 110 003, India.

Tel: +91 (11) 24644693, 24644763, 24620130
Fax: +91 (11) 24647093
Email: guidepub@vsnl.com

POSTAL ADDRESS
Post Box No 2525
New Delhi 110 005, India.

REPRESENTATIVE OFFICE
BANGALORE, INDIA
534, Jal Vayu Vihar
Kammanhalli Main Road
Bangalore 560043, India.
Tel: +91 (80) 23682534

www.spguidepublications.com

Word from the Editor

Information technology can really synergise and optimise the combat power, simultaneously making the decision making process easier and sensor-to-shooter time shorter. In concept, Command, Control, Communications, Computers, Information and Intelligence (C4I2) is simple. Airborne, space-based, underwater and surface-based sensors provide information through surveillance and reconnaissance. This information is then converted into intelligence which is used for faster decision making, enabling effective command and control. Computers provide automation, rapid collation of information and converting it into intelligence resulting in faster and accurate decision making. Reliable and secure communications is the backbone of C4I2.

In practical terms, the establishment of such a network presents daunting challenges. Deliberating on such a micro-niche subject demands a thorough understanding of the key parameters, structural framework and operational criteria—a kaleidoscopic tapestry that could be exhaustive in scope yet invariably engrossing in content. SP's Special Supplement for this unique and quite unprecedented C4I2 Summit covers all facets of this very important war fighting tool. A treatise on TAC-C3I brings out the broad Indian perspective and outlines the future for Indian war fighters.

Even as the focus is firmly on the technology shift of C4I2 product lines from 'Hardware Centric' to 'Software Centric' to 'System Centric' to 'Network, cyber security is extensively discussed, with the stress being on preparedness and vigilance. Yet another key equipment in E-vigilance and situational awareness are sensors that, with extensive data links, can operate effectively in intense electronic traffic.

In the Indian context, the Indian Air Force (IAF) has deployed legacy radar systems like Indra, ST 68 and P-18. The IAF has also started deploying EL/M -2083 tethered Aerostat Radar Systems ex Israel. The much awaited Airborne Warning and Control Systems aircraft finally arrived from Israel in May and will provide a quantum leap in the quality of air surveillance. With homeland security of prime importance, it is only apt to showcase the vital role played by C4I2 in ensuring alertness to danger 24x7. All in all, there's no denying that service-based C4I2 solutions can improve operational capabilities for net-centric defence strategy.

Acknowledgements are due to the entire editorial and layout design team of SP's, under the guidance and stewardship of Senior Managing Editor Air Marshal (Retd) V.K. Bhatia, for burning the midnight oil to ensure the supplement captures every single nuance of the subject under discussion.

Congratulations to the organisers Network18 for providing this excellent platform for industry pundits, scientific minds, military top brass, OEMs and distinguished academic personalities to interact and exchange valuable information on this critical facet of modern warfare. We hope readers will synergise the articles in the supplement and the presentations at the summit to derive full benefit.

Jayant Baranwal
Publisher & Editor-in-Chief

MISSION-CRITICAL ADVANTAGES WHATEVER THE MISSION

For more than 40 years, some 300 Bombardier special mission aircraft have been selected by countries around the globe to fulfill a wide spectrum of missions ranging from government VIP transportation, through search and rescue, to C4ISR. Today, we continue to meet the critical needs of governments, armed forces and commercial operators with high performance Global, Challenger and Learjet series jets and Dash-8/Q-series turboprops. We meet your needs. We deliver.

BOMBARDIER

FOR MORE INFORMATION: WWW.SPECIALMISSION.BOMBARDIER.COM

IAI introduces the POP-300D (Designator)

Israel Aerospace Industries (IAI) has launched the newest member of its POP EO/IR payload family: the POP-300D designator (Plug-in Optronic Payload 300 Designator). The POP-300D, part of the POP family of advanced, lightweight, single Line Replaceable Unit (LRU), observation and targeting payloads, places a concentrated laser spot on a target of interest, enabling precise homing of laser guided munitions on such targets. The POP-300D provides day and night reconnaissance and surveillance capability, together with a dual band laser that enables target designation and range finding. The POP-300D also supports most NATO laser guided weapons.

Lockheed Martin buys small surveillance system firm

Lockheed Martin's planned purchase of Gyrocam Systems is the latest in the ongoing trend of major prime contractors acquiring firms with niche technologies that have future growth potential. Gyrocam is a privately-owned company with 160 employees that makes gyro-stabilised optical surveillance systems that combine infrared, high-definition, night vision and laser range-finding imaging capabilities for ground vehicles and stand-alone platforms. Lockheed announced the agreement on July 22, but didn't disclose the purchase price.

Saab and Swiss UAV team up on Rotorcraft

Swedish aerospace company Saab has struck a deal with Swiss UAV to collaborate on the development and marketing of rotorcraft unmanned air vehicles. The deal merges Saab's Skeldar and the smaller Swiss Neo and Koax into a single family of helicopter UAVs. It is expected that the vehicles will find applications in military and civilian markets capitalising on Saab's ground control expertise.

Raytheon awarded deal for Space Fence System design and prototyping

Raytheon Company has been awarded one of three contracts for Phase A system design and prototype of the Space Fence system. Space Fence will provide the US Air Force enhanced space surveillance capability to detect and report space objects. The Space Fence programme is a multi-phase acquisition leading to the delivery of up to three globally positioned S-band radars capable of interoperation with the Space Surveillance Network.

Northrop Grumman highlights UAS at UVEurope 2009

Northrop Grumman has a 60-year history of providing more than 100,000 unmanned aircraft systems to military customers in the US and around the world. Northrop Grumman exhibited at UV Europe the Global Hawk high altitude long endurance unmanned aircraft including the US Navy Broad Area Maritime Surveillance Unmanned Aircraft System, the German Luftwaffe Euro Hawk (r), the NATO Alliance Ground Surveillance unmanned airborne segment, MQ-8B Fire Scout vertical take-off and landing unmanned aircraft, the X-47B Unmanned Combat Air System and the medium altitude, extended range MQ-5B Hunter unmanned aircraft.

Defence Agency awards Raytheon contract to develop an Interoperable Network Gateway

Raytheon Company has been awarded a contract by the Defence Advanced Research Projects Agency to provide a cost-effective, highly capable military wireless network interoperable gateway. The contract provides Raytheon $24.4 million for one year. Options would extend the contract to 2012 and bring the potential value to $155 million. The Mobile Ad-Hoc Interoperability GATEway, or MAINGATE, will integrate any combination of heterogeneous military, civil or

DRS Tactical Systems

RVS-330

Scorpion Laptop

Military Rugged Tablet

DRS Tactical Systems (DRS-TS) is the world's leading supplier of Battle Management System (BMS) rugged computer and display systems. DRS-TS is a part of the US company DRS Technologies, a wholly owned subsidiary of Finmeccanica s.p.a. Significantly, Finmeccanica is also the supplier of Battle Management System computers and displays to the Italian MoD. DRS has been selected to provide BMS hardware by:

- US Army, FBCB2
- US Army, Blue Force Tracking (BFT)
- US Army, Movement Tracking System (MTS)
- US Marine Corps, Blue Force Tracking
- UK Ministry of Defence, BOWMAN System

These world-renown & combat-proven BMS systems total more than 120,000 Ultra-Rugged Computers and Displays relied upon by soldiers and commanders for mission-critical performance and reliability.

DRS BMS systems delivered to date include:

- Rugged Battle Management Data Terminal, a 13" Laptop
- Rugged Vehicle Data Terminal, a 12" Dismountable Tablet Computer
- Joint Platform Tablet (JPT) MRT, a 10" Dismountable Tablet Computer with optional SAASM GPS and TACLINK modem with Docking Assembly.
- Commander's Crew Station Display (CCS), a 10" remote display with bezel keys
- JV5, a Three-piece system with remote 12" rugged touch screen display, 1.66 Ghz Core Duo platform server with optional SAASM GPS & TACLINK modem, and external keyboard.

All computer systems feature removable hard drives and MIL-STD qualifications. No company has greater BMS experience, a broader range of proven BMS products, or more BMS systems in the field than DRS Technologies & Finmeccanica. ■

coalition radios into a single network to facilitate communication among disparate systems.

Lockheed Martin to continue development of secure information sharing system for US Navy

The US Navy has awarded Lockheed Martin an indefinite-delivery indefinite quantity) contract to continue the development of Radiant Mercury, a secure Multi-National Information Sharing system used by the DoD. Considered to be one of the premier cross-domain solutions, Radiant Mercury is a critical component of many security domains used by DoD, national intelligence agencies, as well as US coalition partners. The contract entails field support for 483 Radiant Mercury systems worldwide, as well as continued enhancement to the system's capabilities.

Northrop Grumman's Global Hawk crosses 31,000 cumulative flight hours

RQ-4 Global Hawk UAS, built by Northrop Grumman Corporation, continues to prove its mettle by exceeding more than 31,000 cumulative flight hours for the US Air Force and US Navy. More than 76 per cent of these flight hours were flown in support of overseas contingency operations efforts.

FBI awards Lockheed Martin biometric card scanning service contract

FBI has awarded Lockheed Martin a five-year; $47 million contract to continue managing the FBI Criminal Justice Information Services (CJIS) Division's Card Scanning Service programme. The contract covers the conversion of paper fingerprint, palm print and photo records into high-quality electronic records for the FBI. Records processed through this programme are submitted by state, local, and federal law enforcement agencies and used to populate the Integrated Automated Fingerprint Identification System database, a national fingerprint and criminal history system maintained by the FBI CJIS Division.

Boeing awarded production contract for US Air Force AWACS Block 40/45 upgrade

The Boeing Company has announced that it has received a Low-Rate Initial Production contract for the Block 40/45 upgrade of the US Air Force AWACS fleet. Boeing will provide shipset hardware, spare parts, ground systems installation, and delivery and logistic support for the first aircraft to undergo the upgrade. The Block 40/45 upgrade will dramatically enhance the system's potential for using network-enabled operations and increase AWACS mission execution capability.

SELEX Galileo introduces an easily deployable integrated surveillance system

SELEX Galileo of Finmeccanica has recently presented to the Italian Navy and to a delegation of the Italian Army the new TPS - 730 radar integrated with the electro-optic turret NEMO at the UTT Nettuno Range. SELEX Galileo has developed the TPS - 730 radar integrating it in an "all in one" shelter, including a telescopic pole for the Antenna and the NEMO electro-optics. This system can be easily transported and deployed in Homeland Security and Protection scenarios.

Terma integrates Danish Air Force upgraded TRS program

The RDAF's Tactical Reconnaissance System (TRS) has been subject to an upgrade programme to become NATO STANAG compliant. L-3 Communication Systems-East's S/TARTM RM-4000T Solid State Recorders was selected for its commonality with the US ANG F-16 TARS programme and its compliance to STANAG 4575. Terma was responsible for the integration of the new recorder into the TRS pod and for all ground testing. The successful flight testing was performed by the RDAF in cooperation with Terma. The Danish Defence Acquisition and Logistics Organisation reported they are pleased with the rapid installation performed by Terma in cooperation with L-3 Communication Systems-East.

IAI Heron UAS demonstrates advanced capabilities

Israel Aerospace Industries (IAI) and a Spanish company have held a joint demonstration of IAI MALAT Division's maritime Heron UAS. The demonstration portrayed the Heron's abilities to successfully patrol, detect, classify and identify maritime targets of all types. The Heron UAS was operated by teams from IAI, while the command and control system was operated by the Spanish company. The early detection of boats and vessels, some of them very small, carrying smuggled goods or illegal immigrants, is an important need for European Union countries.

Boeing bags USAF contract to demonstrate Cyber Command & Control solutions

Boeing was recently awarded a contract by the US Air Force Research Laboratory to study and demonstrate improved situational awareness, visualisation, and automated course-of-action processing for network environments during cyber attack. Boeing will analyse network operations, develop procedures and processes, and apply tools that will enhance network command and control capabilities.

Northrop Grumman's second E-2D Advanced Hawkeye enters next phase of testing

Northrop Grumman Corporation's second E-2D Advanced Hawkeye, known as Delta Two, has transitioned to Naval Air Station Patuxent River carrier suitability phase of testing. Designed and built for the US Navy, the E-2D will utilise its newly developed AN/APY-9 Electronic Scan Array radar, Cooperative Engagement Capability system, Electronic Support Measures , and off-board sensors, in concert with surface combatants equipped with the Aegis combat system to detect, track, and defeat cruise missile threats at extended ranges.

Northrop Grumman completes first flight of land-based MQ-8B Fire Scout

A Northrop Grumman Corporation's MQ-8B Fire Scout Vertical Unmanned Aircraft System (VUAS), designated P7, has successfully completed first flight operations. Unlike current navy configured Fire Scouts, P7 was built in an operational land-based configuration. It is the first MQ-8B to fly without flight test instrumentation normally installed for developmental flights.

Rockwell Collins selected to provide ad hoc networking for Canadian Navy

The Canadian Department of National Defence has selected

Rockwell Collins to provide Sub-Net Relay Controllers, High Speed Modems and Very High Speed Modems for the Sub-Net Relay (SNR) programme. The contract is valued at $7 million. The SNR technology makes it possible to establish ad hoc, Internet-Protocol networks used for tactical data exchanges, enhanced situational awareness and collaborative planning by the Canadian Navy and coalition navies. Features of the SNR programme include built-in text chat, comprehensive signal display and a remote control graphic user interface.

SELEX Galileo wins contracts for the Italian-French FREMM programme

SELEX Galileo was awarded orders for its sensors solutions for the FREMM frigates of the Italian Navy, the Marina Militare. The total participation of SELEX Galileo, Finmeccanica group, in the programme is now valued at more than €42 million, with the initial contracts dating back to 2007.

IAI's POP-300LR Observer for European Coastal Surveillance Programme

The Plug-in Optronic Payload 300-Long Range (POP-300LR Observer), produced by Israel Aerospace Industries, has been selected by a European customer for use in a costal surveillance programme. The POP-300LR will be integrated with radar and will provide the customer with 24/7, all weather long range observation and surveillance capabilities. The POP-300LR is the ultimate solution for ground applications such as site control, border security, and coastal surveillance, as well as for naval platforms and aerostats that demand cost effective long range object engagement.

General Dynamics form JV to provide Tactical UAVs to US

Elbit Systems Ltd has announced that its subsidiary, Elbit Systems of America, LLC and General Dynamics Armament and Technical Products have formed a new joint venture named UAS Dynamics, LLC, to provide UAS to the Department of Defense and other potential US government customers. The new platforms will fill current and future operational gaps allowing intelligence, surveillance and reconnaissance capabilities that range in size and scope from hand-held and tactical level systems to medium altitude, long-endurance level systems.

Northrop Grumman delivers second demonstration satellite

Northrop Grumman Corporation has completed delivery of both Space Tracking and Surveillance System (STSS) demonstration satellites. Using onboard sensors capable of detecting infrared and visible light, STSS will become part of land, sea, air and space based sensors for the nation's Ballistic Missile Defence System. Once operational, STSS will demonstrate the key functions of a space-based sensor, passing missile tracking data to missile defence interceptors with the accuracy and timeliness necessary to enable successful intercept missile targets.

Raytheon completes acceptance testing for Intelligence-Sharing Backbone

Raytheon Company's Distributed Common Ground System (DCGS) Integration Backbone, or DIB, team has completed a rigorous, multiple-day test of its new DIB version 1.3, representing an important step toward delivering new intelligence-sharing technology to users worldwide. DIB software is installed in more than 100 systems around the world.

EADS Defence & Security highlights advanced UAV

At the Paris Air Show 2009, EADS Defence & Security (DS) presented the mock-up of their latest UAS (called Talarion), a joint programme of France, Germany and Spain which is a fully autonomous system for Intelligence, surveillance, target acquisition and reconnaissance missions.

DRS Technologies receives US Army order for Infrared Sighting Systems

DRS Technologies, Inc. has announced that it has received a follow-on order for Second Generation Forward Looking Infrared sighting systems and components from the Raytheon Company's Network Centric Systems. The systems are to be fitted onus Army tanks and combat vehicles.

Elbit Systems US subsidiary, General Dynamics form joint venture to supply tactical UAVs to US

Elbit Systems Ltd has announced that its subsidiary, Elbit Systems of America, LLC and General Dynamics Armament and Technical Products have formed a new joint venture named UAS Dynamics, LLC, to provide unmanned aerial systems to the Department of Defense (DoD) and other potential US government customers through programmes such as the recently announced US Marine Corps' Small Tactical Unmanned Aircraft System /Tier II programme.

Finmeccanica part of pact for Eurofighter Typhoons

Finmeccanica has announced that NETMA (NATO Eurofighter and Tornado Management Agency), Eurofighter GmbH and EUROJET Turbo GmbH have signed a further production contract for the Eurofighter Typhoon aircraft. The contract, worth a total of € 9 billion, relates to a third tranche production for 112 aircraft. €3 billion of the contract value pertains to Finmeccanica and includes the industrial activities such as defining, designing, developing and producing the aerostructure, systems integration and avionics for the aircraft.

Telespazio (Finmeccanica/ Thales) and Turkish Defence Ministry ink contract to build Göktürk satellite system

Telespazio, a company owned by Finmeccanica and Thales, and Undersecretariat for Defence Industries (SSM-Turkish Defence Ministry), have signed a contract in Ankara for the construction of the Göktürk satellite system. The agreement covers the supply of an earth observation satellite equipped with a high-resolution optical sensor, an integration and test centre for satellites to be built in Turkey, and the entire ground segment of the system, which will carry out in-orbit operation, data acquisition and processing.

ITT announces image processing product for GIS professionals

ITT Corporation, the developers of ENVI image processing and analysis software, and ESRI,

IAI-ELTA's Special Mission Aircraft - At the Core of Intelligence Collection, Battle Management & Homeland Security Operations

- Signal Intelligence (COMINT & ELINT) & Tactical Electronic Support
- Conformal Airborne Early Warning & Control (CAEW)
- Image Intelligence (Synthetic Aperture Radar & Electro-Optics)
- Maritime Patrol
- Advanced communication systems (LOS & SATCOM) for net-centric operations
- Long endurance, high altitude business jet or advanced turbo-prop platforms
- Onboard & ground C^4I Centers for mission control, situation awareness & intelligence report dissemination

IAI-ELTA's Special Mission Aircraft always put you in control. Our Record Proves it.

IAI
ELTA SYSTEMS

Israel Aerospace Industries | **E-mail: market@elta.co.il** | **www.elta-iai.com**

the leading provider of GIS software, ArcGIS, have announced a strategic partnership to integrate their respective software technologies. This integration delivers advanced, high-performance image processing and analysis capabilities to the ArcGIS platform and expands the distribution of these new technologies globally.

ThalesRaytheonSystems receives approval for replication of NATO Air Command and Control System Level of Operational Capability program

Currently deployed at five sites in Belgium, France, Germany, Italy and the Netherlands, ACCS LOC 1 will replace NATO's existing air command and control systems in Europe and set new standards of interoperability for air operations with a single, integrated approach to planning, tasking, monitoring and mission execution. ACCS LOC 1, NATO's largest-ever software system, uses open-system architecture to adapt to changing operational requirements, such as theatre missile defence and network-centric warfare. When fully deployed, NATO member countries will be able to share operational data over a high-speed communication system.

Raytheon adapts Common Ground System to KillerBee UAS

Raytheon Company has tested a proven, open-software architecture unmanned ground system that enables one ground station to control multiple KillerBee UAS. "We have taken a ground system, which is a variant of the US Navy's Tactical Control System and adapted it to a Linux operating system to make it hardware independent and fully scalable," said Mark Bigham, Raytheon Intelligence and Information Systems business development director. In a recent demonstration, Raytheon controlled the KillerBee aircraft while simultaneously providing manned, anti-tank guided weapon target information from the aircraft which significantly shortens the kill chain.

Germany paves way for Afghan AWACS deployment

German politicians are backing deployment of the NATO AWACS for missions over Afghanistan. NATO has announced its decision to deploy the aircraft during a meeting in Brussels on June 12. The crew of each NATO E-3A AWACS can include up to one-third German personnel but the final decision has to be taken by the German Bundestag. The German government has agreed in principle to send an additional 300 personnel to support the AWACS deployment.

Successful first campaign of flight tests for Patroller surveillance UAV

Sagem (Safran group) and Stemme have successfully carried out the first campaign of flight tests for the Patroller long-endurance surveillance UAV system, scheduled to be qualified in 2010. The campaign was carried successfully over 8 flights, including a flight lasting more than 10 hours. Patroller can fly 30 hours in autonomous mode at an operational altitude of 25,000ft and with a maximum speed of 300 km/h. Patroller has an image chain based on Sagem's Euroflir 410 gyrostabilised optronic observation system and a Synthetic Aperture Radar pod from OHB. Down the line it will be able to carry other payloads.

Russia buys Israeli UAVs to study capabilities

In a rare case of buying foreign defence items for its military, Russia has acquired 12 UAVs from Israel for $53 million. The main goal of the purchase was to study Israeli technology in order to build drones in Russia. However this approach has irked Israeli defence officials who told Israel's Jerusalem Post newspaper in comments published June 23 that Israel would not sell Russia its most advanced drones.

BAE Systems delivers 100,000th uncooled infrared thermal imager

BAE Systems recently delivered its 100,000th MicroIR uncooled thermal imager, which will be installed in the US Army's Common Remotely Operated Weapon Station (CROWS II). The thermal imagers detect heat from people, vehicles, and other sources enabling soldiers to identify targets while remaining protected inside their vehicles. The MicroIR devices work in darkness and in smoke, fog, and other visibility-obscuring conditions. Unlike other infrared sensors that require cryogenic cooling, the MicroIR devices require no cooling and therefore are smaller, lighter, and use less power.

New unmanned baby sub to protect coastal waters

In a move to help combat the growing threat of explosive mines hidden in shallow coastal waters such as ports and harbours and to increase the protection available to world shipping, BAE Systems has launched its first unmanned autonomous submarine to detect and deal with this newfound threat. The 50 kg vessel, called Talisman L, uses high-definition forward and sideways looking sonars, as well as a host of multi-view cameras.

Italy Defence Minister promises more UAVs, helicopters

Ignazio La Russa, Italy's Minister of Defence, has promised Italian soldiers in Afghanistan more UAVs and suggested that more helicopters also could be on their way. La Russa said in Herat on July 21 he would send more unarmed Predator UAVs for surveillance missions. Italy already has acquired two upgraded Predator As to join the four it has in service, and is purchasing four unarmed Predator Bs.

European Defence Agency mulls biological protection

The defence ministries of the EDA member countries have approved a €100 million ($135 million) demonstrator project for force protection against biological agents, called the Biological Detection Identification Monitoring Equipment Development and Enhancement Programme. So far five countries - the Czech Republic, France, Germany, Netherlands and Spain - are due to contribute €20 million each.

Raytheon, NGA improve flow of commercial imagery to warfighters and analysts

Raytheon Company and the National Geospatial-Intelligence Agency (NGA) marked the transition of an improved capability that will rapidly ingest and disseminate imagery from US commercial satellite companies to warfighters and intelligence analysts worldwide. The effort was related to the agency's NextView programme, in which NGA receives imagery from US commercial satellite companies. With the new dissemination capability, NGA systems can now ingest and disseminate greater amounts of commercial satellite imagery daily, providing it to users more quickly. NGA has also tasked Raytheon to provide the next generation of services to disseminate data from multiple sources to its users. ■

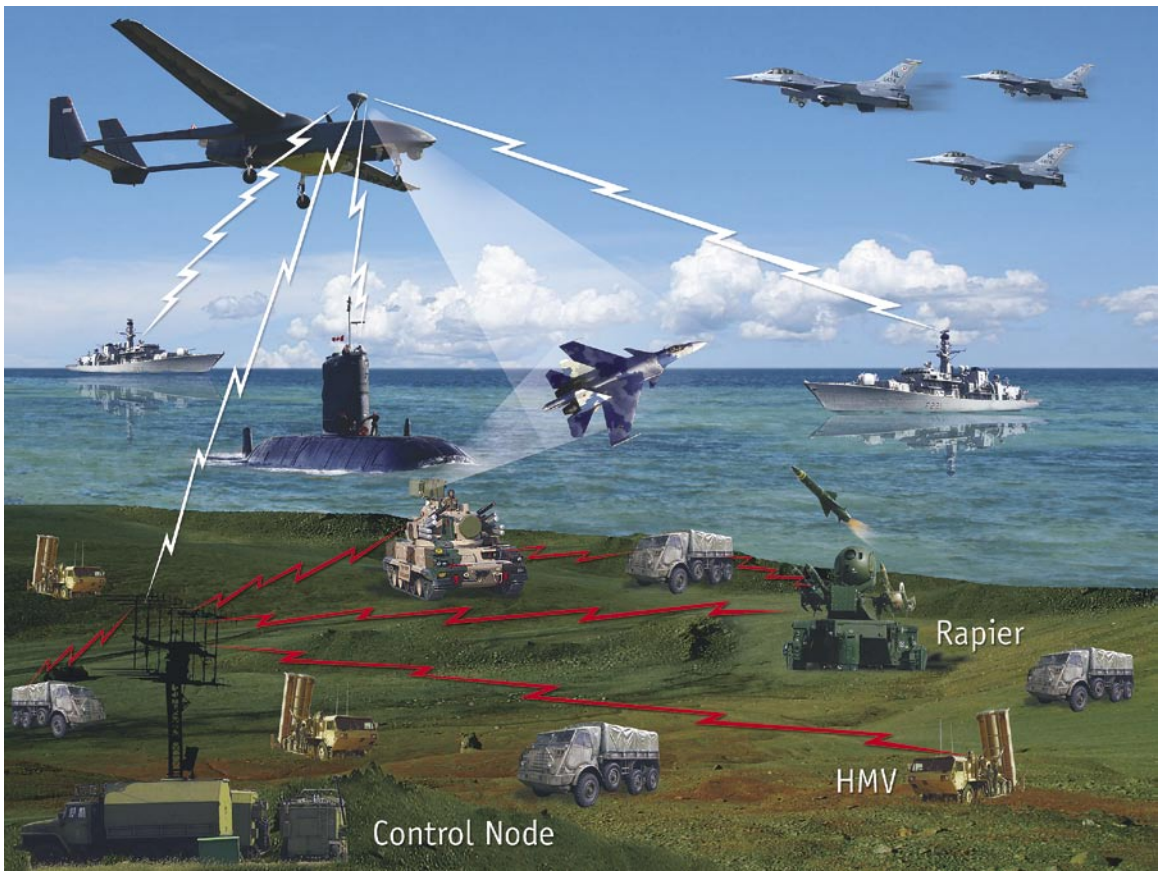


ILLUSTRATION: RATAN SONAL

Essential RMA Enablers

There is a need to create a seamless link from the bottom to the top. At the core is ASTROIDS, below which is the TAC-C3I system—its fulcrum being the Command Information Decision Support System

By **Brigadier Vinod Anand & Anil Singhal**

To respond effectively to the 21st century battlefield requirements, the Indian Army needs to engineer change. At present, it is in a transitional phase of moving from industrial age type of warfare to information enabled warfare, that is, from platform centric to network centric warfare. Transformation should help it in adapting to Revolution in Military Affairs (RMA) and Network Centric Warfare (NCW). Throughout this process of change, the requirement for Information Superiority and Information Assurance will remain an imperative across the entire force.

The separator between tactical, operational and strategic levels of warfare is blurring. While there was always some degree of overlap between these levels, owing to the increasingly pervasive influence of information technology (IT) on warfare this overlap is increasing. On account of this blurring of distinction between the levels of warfare, the Observe, Orient, Decide, and Act (OODA) cycle has to be traversed much faster. In effect, we have to break the opponent's OODA cycle and ensure quicker action while the enemy is kept disoriented.

There is a need to create a seamless link from the bottom to the top as an integrated army enterprise. At the core of this enterprise is the Army Strategic Operational Information Dissemination System (ASTROIDS) which will connect Army HQ with the various theatre commands and downwards to the operational corps. A C4I2 (Command, Control, Communication, Computers, Information and Intelligence) system above corps level has been evolved; ASTROIDS is to be the operational system between the national level and army authorities.

Functioning below ASTROIDS is the Tactical, Command, Control, Communication and Information (TAC-C3I) system. Designed as the primary functioning system for the field formations, TAC-C3I, in turn, has other components under design. The fulcrum of which is going to be the Command Information Decision Support System (CIDSS).

AIM OF TAC-C3I SYSTEM

The TAC-C3I system is designed to assist in planning, directing and controlling field forces whose function it is to provide:

- Commanders at all echelons with accurate, timely and credible information
- Means to process, display and evaluate data for situational awareness as an aid for decision support, and
- Capabilities to transmit order and decisions to own forces and weapon systems both during war and peace

Relevance of the C3I in the field of modern warfare is constantly growing. The future forces would have to be highly mobile and technologically superior to the enemy. Hence, technological advancement is required to enhance the war fighting potential at strategic, operational and tactical levels. The analysis and usage of information is as important as information collection through different sources to derive the situational awareness. C3I is an important prerequisite for NCW. Increased level of battlefield transparency would ultimately turn commanders (decision makers) into 'Battlefield Managers'. They would operate from their network of systems enabled control rooms.

TECHNICAL OBJECTIVES

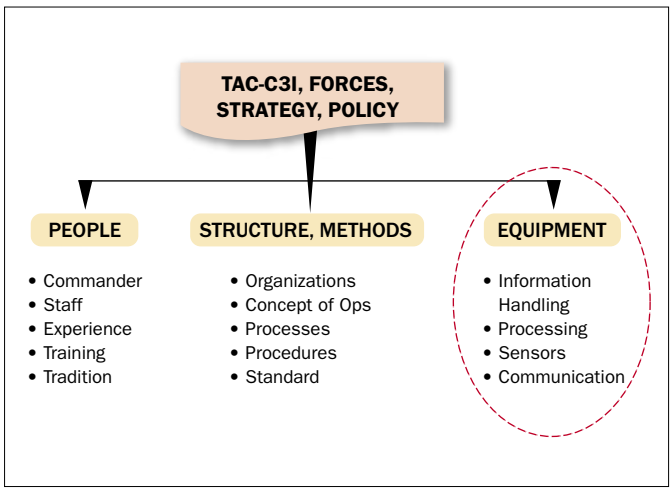
The key technical objectives of the TAC-C3I system are based on the principles of:

- One time data capture
- Managing data separately from applications
- Standardising and sharing data throughout the TAC-C3I
- Creating a centrally managed but distributed database environment
- Establishing standard application development environments for all components of TAC-C3I
- Computer supported evaluation of data to arrive at Common Operational Picture for rapid decision making
- Rapid transfer of information between units for effective command and reporting.

COMPONENTS OF TAC-C3I

A typical TAC-C3I is a system made up of people, procedures, equipment and information systems as depicted below:

Typically C3I systems are viewed only as the equipment part (shown in dotted circle) and ignore the other two components, thus resulting in partial effectiveness of the TAC-C3I system.



VARIOUS TAC-C3I PROJECTS

During the 1990s, the Indian Army fielded the TAC-C3I, Management Information Systems and Geographical Information System. Development and fielding of automated operational and information systems for various levels of operations from Corps Headquarters to Battalion headquarters to individual soldiers are in progress as part of TAC-C3I systems as under:

- Command Information and Decision Support System
- Artillery Command, Control and Computer System
- Battlefield Support System (BSS)
- Air Defence Control and Reporting System
- Air Support System
- Air Space Management System, and
- Electronic Warfare System

PROJECT SAMVAHAK

It is being developed by the Defence Research and Development's Centre for Artificial Intelligence & Robotics (CAIR) as the lead lab/nodal agency, who in turn sought help from the industry. Tata Consultancy Services was awarded software part of the phase 1 contract which has been fielded in nominated corps with hardware outsourced from the industry.

The plan is to implement the TAC-C3I System by developing and cohesively integrating the components shown in diagram below:

Problem in such system development occurs due to the different perception held by users, coordinators (PMO) and nodal developers, which tend to get resolved over a period of time by understanding each other's constraints. Project Samvahak's CIDSS aims at:

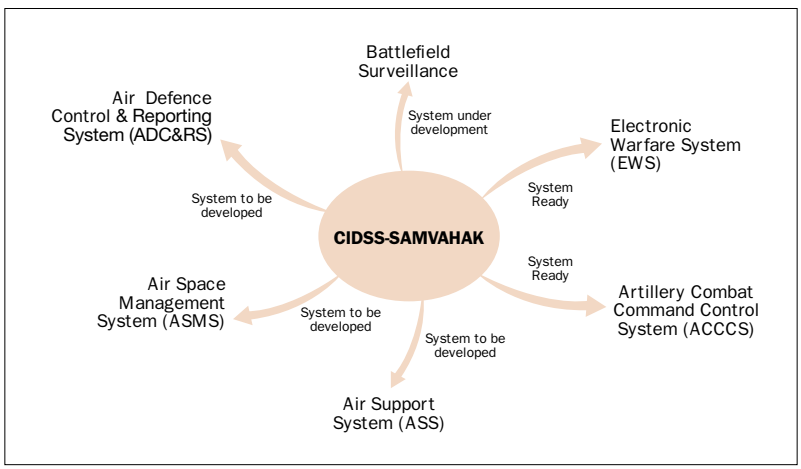
- Collecting, collating, filtering, processing, formatting and displaying operational, intelligence and logistics information to the commanders to enable them to take appropriate and timely decisions.
- Presenting decision options to commanders and supporting dissemination of decisions, plans, tasking and operational orders.

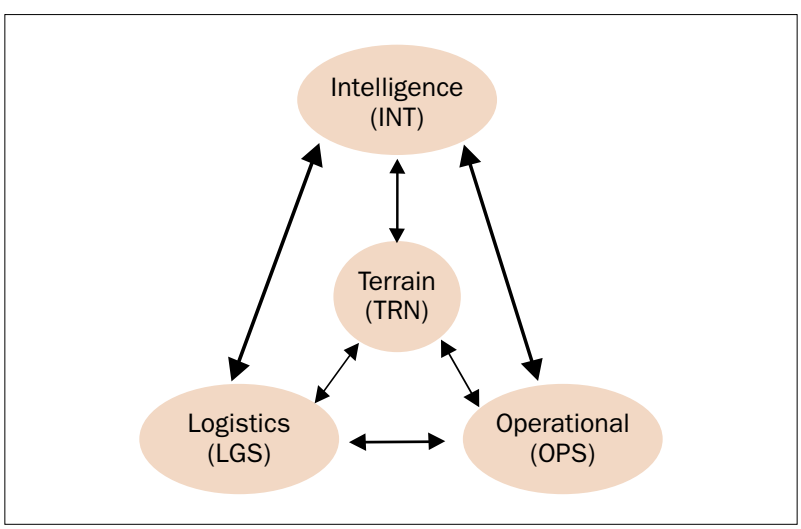
CIDSS SUB-SYSTEMS

The CIDSS System comprises of four subsystems which are

based on similarity of functions of a field force as shown in diagram below:

CIDSS was conceived as an umbrella structure to optimise decision-making and is expected to network all other automated systems. Currently, TAC-C3I projects are in various stages of development and fielding. These projects were developed independently by different PMO. Subsequently, the requirements of intra-service interoperability were realised. Based on the TAC-C3I vision; attempts are being made to achieve fair degree of interoperability by 2012. Vertical integration with various sub-systems and development of standard protocols to facilitate integration is also under process and will be put in place soon. Integrated together with requisite communications, these systems will provide near real time 'Sensor-to-Shooter' links to make army a network-centric force.





MODELING & PERFORMANCE EVALUATION

The Indian Army had fielded the CIDSS (Samvahak) in Exercise Parikshan, Exercise Akrosh and Exercise Vajra Shakti for Indian army commanders. The army has also tested Sanjay situation assessment tool as part of BSS. It has been claimed that both Samvahak and Sanjay have robust information security features.

The functions of any element of a complex system must be understood, modelled and quantitatively evaluated to determine the contribution that it provides to the effectiveness of the C3I system. This process of quantitative assessment is often applied to the elements of TAC-C3I systems to determine the contribution it provides to the military effectiveness of those systems.These assessments are required to answer important system-level issues that are frequently raised to satisfy the users at all levels. The methods to model C3I systems, define measures of merit to quantify performance and effectiveness, and conduct tests and analyses to explain the results must be understood and applied.

The intrinsic characteristics of a TAC-C3I system are as follows:

- The unique requirements of the C3I system users will keep evolving. Hence, there will always be significant amount of proliferation in the applications that are going to be developed. This necessitates the need for a mechanism to integrate new applications into the TAC-C3I system configuration as it matures. Development plateform be based on Open systems.
- The development time and costs for C3I systems are high because of the sheer size of the system. So these need to be reduced by usng commercial off-the-shelf components and technologies to evolve cost effective solutions.
- Project Samvahak focuses mainly on the equipment aspect, hence it is not a panacea to the desired state required to be achieved as far as an effective decision support system is concerned. There is an urgent need to integrate this with the other aspects as shown in the above diagram. Full realisation of any such revolution is possible only with technological development, organisational adaptation, and most importantly a strong defence and national will.

DIGITISATION ASSESSMENT

There is a need to monitor battlefield digitisation efforts until the digitisation hypothesis has been demonstrated and core functionality achieved. Core functionality is the minimum set of capabilities that permit the user to effectively accomplish his mission in the expected operational environment. Further, core function-

ality should include sufficient levels of interoperability, logistics supportability, life-cycle support, survivability, and training adequacy, such that the user would be satisfied if no additional capability were ever delivered.

Despite the significant improvements observed, the current state of digitisation capabilities is not sufficient, with a number of critical enhancements necessary to achieve an effective and suitable capability. These include a robust speedier network and its management capability to monitor the network's health and respond to identified problems, improved interoperability within and across the Army.

ROAD AHEAD

Not only must we continue to support current initiatives on priority, but we must also plan for the road ahead. It is important to realise that 'Information Assurance' requires a holistic approach with continuous training and maintenance. We must continue to develop the synergy between the policies, personnel, procedures, and tools in the future.

A road map has been formulated by which we can progress steadily towards being a potent IT force. Development of C3I systems has been identified as a major thrust area for modernisation of army. Development and fielding of automated operational and information systems for various levels of operations from Army Headquarters to Battalion Headquarters to individual soldiers are in progress. There is enough importance and urgency from the end users but procedural delays are happening beyond their control. There is a need to give priority to the First Digitized Division and First Digitized Corps where tactical C3I systems have been fielded.

India needs to integrate new technologies as warfighting systems for which the requirement is to simultaneously evolve a new joint warfighting doctrine and concepts of joint warfighting and then decide upon the weapons and other systems to suit the former, integrated as part of the TAC-C3I system.

Employment of joint/integrated task forces in the future would require, introduction of three critical technologies as under:

- Long Range Precision Firepower supported with requisite terminal guidance
- Integrative Technologies (like, C3I and C4I2), and
- Intelligence, Surveillance and Reconnaissance

The progress made for acquiring the above systems and technologies has been extremely slow. India needs to take advantage of the new found friendship with the US and the western world to acquire hardware and technologies from abroad if the country's scientists cannot develop them.

STRENGTHS & CHALLENGES

Despite having so many advantages and potentials, the TAC-C3I system is not free from problems. C3I is mainly a computer-based network; therefore, it has several difficulties such as inherited problems of the network, content retrieval, data mining, context awareness, tactical manifestation as 'information overload', possibilities of excessive accumulation of irrelevant information and key information loss.

The system cannot decipher relationships between information and may hence prove incapable of flashing the key information within the sensor-to-shooter loop. Whatever be the shortcomings, the fact remains that C3I is possible and achievable with cutting edge technologies, and to act as a force multiplier.

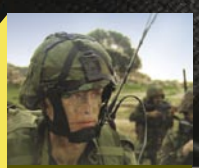
To maintain information superiority, digitised systems must keep pace with technology. There is a need to be able to insert modern technology into existing systems rapidly. With Moore's Law accurately predicting a doubling of processing power every 18 months, this demands a revision of our acquisition methods. The development cycle itself must be in short spirals with 'Beta' releases of software for user assessments in operational environments before full system maturity is reached.

To maintain information superiority, digitised systems must keep pace with technology. There is a need to be able to insert modern technology into existing systems rapidly.

IT will enable the armed forces to dominate future battlefields. But this technology is also vulnerable to attack and exploitation. Consequently, we must build and sustain a robust information assurance programme to provide defence-in-depth. Both China's and Pakistan's anti-technology designs are heightening the concerns of the world. China recognises that to be a great power, it has to dominate all areas including ICT and NCW. Consequently, Beijing has created and deployed very potent cyber warfare units. The Chinese have launched cyber attacks on official sites of tech savvy and developed countries like the US, France, Germany and England. Recently, they tried a similar tactic on India also, highlighting the need to develop techniques to fight NCW effectively

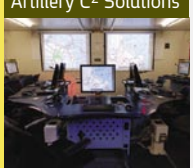
The adoption of a powerful concept, process, method, and/or tool often holds promise of dramatic benefit to an organisation. However, efforts to realise these benefits often result in frustration and resistance from those who should receive the benefits. Previous problems with adoption have convinced many to take a very conservative 'wait and see' attitude about new technology. Such conservative strategies may reduce the downside, but in today's hyper-competitive world, they may also make it impossible to survive. Mastering the adoption of new technology may indeed separate the winners from the losers. ■

NEW TOOLS FOR NEW RULES

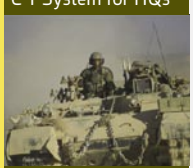


DOMINATOR®
Integrated Infantry
Combat System

Artillery C2 Solutions



TORC2H®
C4I System for HQs



WINBMS - Weapon
Integrated Battle
Management System

Networking the Land Forces in the Information Age

Elbit Systems creates and implements net-centric solutions of Land Force C4I. This spans every level of command and activity from soldier solutions to National Headquarters and all echelons in between, enabling the real time exchange of data and information supporting all battlefield, logistic and operational functions.
Forces can now achieve previously impossible levels of situational awareness, interoperability and coordination.
Elbit has made communications a key force multiplier, getting more from the same fighters and equipment than ever before.

Elbit Systems
Land and C4I - Tadiran

NEXT IS NOW™
www.elbitsystems.com

Act on the Intent

The possibility of cyber warfare should be treated asseriously as the threat of a missile strike. The answer lies in preparedness and vigilance.

By **Lt General (Retd) S.R.R. Aiyengar**

In the current digital era, wherein 'governance' as well as 'business' is increasingly being dictated by information and communication technology, any deliberation on security of the nation is not complete without a discussion of the cyber space in which E-governance and E-commerce take place. Attention is usually drawn to cyber security when news about cyber crimes emerges. Any cyber attack can have serious and expensive repercussions, be it targeted towards individuals, small business or corporations. Intellectual property can be compromised, personal and business information can be stolen, normal business operations can be disrupted and major financial losses can occur.

More seriously, attacks on the government machinery carry the increased threat of theft of government and military secrets. There is also the real possibility that a cyber attack could disable defence command systems, bring down power grids, open dam floodgates, paralyse communications and transportation, create mass confusion and hysteria. Any or all of which could be precursor to land, sea and air conventional and nuclear military attacks. E-governance and E-commerce sectors, as well as the individuals who use computers and mobiles, are also concerned about cyber crimes and how it affects them. The question, therefore, arises as to what is the role, if any, of the corporate sector or common 'Netizens' in ensuring 'National Cyber Security'.

Compared to any assessable dimension, the parameters of cyber space is somewhat different. While it has no boundaries, it also means that beyond the cyber space of every individual, exists an international cyber space. So every time a 'Netizen' sends or receives a data packet on the Internet, he is venturing out of the national cyber space and wandering into international cyber space. Therefore, civilians and the corporate sector have a far bigger role to play in national cyber space security.

Consequently, the strategy for national cyber space has to be different from that for the physical cyber space. Rapid expansion and global dependence upon cyber space has compelled many countries to evolve their war fighting doctrines to include cyber space as a viable domain at par with the domains of land, sea, air and space. Cyber offence is a thousand times easier than defence—thus, breaches are most certainly occurring in all countries, virtually all the time. Nothing should surprise us.

RESPONSE TO CYBER THREATS

The cyber security shield put in place by the US, a nation highly dependent on automated and inter-connected national infra-

ILLUSTRATION: RATAN SONAL

structures, is worth examining. Pentagon places the highest priority on cyberspace even as US military has moved ahead and created its first 'Cyber Command' designed to bolster America's potential to wage digital warfare as well as defend against mounting cyber threats, The move reflects a shift in military strategy with cyber dominance now part of US war doctrine and growing alarm over the perceived threat posed by digital espionage by China, Russia and other nations. China, as has been widely reported, has built up a sophisticated cyber warfare programme. So much so, a spate of intrusions in the US and elsewhere can be traced back to Chinese sources.

Defence officials say the 'Cyber Command' would focus on security efforts for US networks along with offensive capabilities to ensure "freedom of action in cyberspace" to protect American interests. While the precise details of the US cyber military power remain a secret, it includes technology capable of penetrating and jamming networks, including the classified 'Suter' airborne system, analysts say. The technology has been reportedly added to unmanned aircraft and allows for users to take over enemy sensors to "see what enemy sensors see, and even take over as systems administrator so sensors can be manipulated into positions so that approaching aircraft can't be seen", according to *Aviation Week*. Speculation is Israel may have used the technology in a 2007 air raid against a Syrian construction site.

In the US government, the National Strategy to Secure Cyberspace is a component of the larger National Strategy for Homeland Security. The National Strategy to Secure Cyber space was drafted by the Department of Homeland Security in reaction to the September 11, 2001 terrorist attacks. Released on February 14, 2003, it offers suggestions, not mandates, to business, academic, and individual users of cyberspace to secure computer systems and networks. It was prepared after a year of research by businesses, universities, and government, and after five months of public comment. The plan advises a number of security practices as well as promotion of cyber security education. Following strategic objectives have been identified:

- Prevent cyber attacks against America's critical infrastructures
- Reduce national vulnerability to cyber attacks, and
- Minimise damage and recovery time from cyber attacks that do occur

The government's role in protecting cyber space has been identified as:

- Forensics and attack attribution
- Protection of networks and systems critical to national security
- ndications and warnings
- Protection against organised attacks capable of inflicting debilitating damage to the economy, and
- Research and technology development enabling private sector to secure critical infrastructure

The roles assigned to the Department of Homeland Security in respect to Cyber Security are:

- Develop comprehensive plan for securing key resources and critical infrastructure of the US
- Provide crisis management for attacks on critical information systems
- Provide technical assistance to private sector to recover failed critical information systems
- Provide specific warning information/advice about protective measures/countermeasures, and
- Perform/fund research/development leading to scientific understanding/technology

THE INDIAN INITIATIVE

For the first time, India is mulling establishment of a Digital Security Agency (DSA) to deal with cyber warfare, cyber counter terrorism and security of national digital assets. For too long India has been aspiring to the position of an E-Super Power without addressing the issue of digital security in totality. But that scenario is fast changing. Traditional information security mechanisms are unable to cope with the treat of cyber terrorism or cyber war because the attacks are sophisticated, backed by supply of adequate resources, encouraged by strong non-commercial motivation and with the support of national government resources. There are organised criminal gangs who are patronised by rogue governments who shelter the criminals and their hosting facilities. It is just like the terrorist camps that are supported in Pakistan to train and attack India.

An attempt was made to provide legal backing for conduct of electronic surveillance and bring cyber terrorism to book by the Information Technology Act 2008 (ITA 2008). However, it still needs to be backed by a national cyber security agency which can focus on ensuring security on a national scale in the cyber space. The DSA can be the fulcrum for development of such an agency. First of all, it

can act as a coordinating agency for national cyber intelligence and integrate the activities of cyber crime policing in different states. It can also enter into cyber crime prevention treaties with other countries to ensure international cooperation against cyber terror.

More importantly, when attacks originate from a remote server, following the principle of 'hot pursuit', the rogue servers can be identified and disabled with a counter cyber attack. As a counter intelligence strategy, it can counter hack, plant its own intelligence gathering mechanisms and defend the country against external aggression through cyber space. Some similar roles and tasks as assigned to the US Department of Homeland Security could be examined in the Indian context and can be overseen by the proposed set-up at the national level.

FIRST STEP FORWARD

The government has already set-up the Indian Computer Emergency Response Team (CERT-In) for promoting cyber security and helping organisations recover from computer security incidents. CERT-In has also circulated security guidelines to all government organisations and has posted them on its website. The organisation also conducts regular security workshops for system and network administrators from government, defence, public sector and private sector organisations.

With the passage of Information ITA 2008, CERT-In shall serve as the national agency for performing the following functions of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incidents response activities, and
- Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

LACKLUSTRE LAW ENFORCEMENT

Noted cyber law expert Pawan Duggal says for every 500 cyber crimes, only 50 are reported and just one is registered with the police. A cyber criminal, he adds, is rarely caught. In the few cases where cyber crime cases have been initiated, lack of coordination between different police authorities has frustrated the investigation. In some cases, when the inquiry trail goes abroad, it is reliably learnt that the CBI is not forthcoming with support and investigations reach a dead end. When cyber crimes are committed with mobile network, it is often difficult to convince mobile service providers of their responsibility to assist police in the investigation.

In the private sector, whenever crimes are reported, most companies invariably get more concerned about their own reputation than public good, and more often than not do everything in their power not to register a complaint nor enable a proper investigation. Worse, often softwares are riddled with bugs that ought to have been removed by developers before introducing the system in the cyber space instead of depending on security patches to plug the loopholes in the future. Some software developers take refuge in IPR claims to shield their source codes and prevent the user from making a proper security assessment. Thus, there is a total lack of co-ordination among various agencies.

Instituting an apex body at the national level would ensure better co-ordination and concerted action in cyber defence mechanism. Any policy arrived at would require a clear logic relating perceived states of vulnerability to the desired aim of those defensive policies. Such logic will require the agency proposed to identify those systems and infrastructures critical to the survival of the country and to its social and economic well being.

Instituting an apex body at the national level would ensure better co-ordination and concerted action in cyber defence mechanism

PLAN AHEAD & FAST

In India, efforts to establish a national cyber security strategy have so far been vague. The National Informatics Centre, which has been involved in many E-governance projects and should be a natural choice for ensuring cyber security, does not seem to have made much progress. The Centre for Development of Advanced Computing has been involved in certain research projects, but is not in the forefront of strategising a national cyber security plan. Private sector is concerned mainly with ISO certification. NASSCOM is focusing on building a security organisation for BPOs which is in the early stages of planning.

A serious attempt to develop a national cyber security agency was made five years back when Dr Abdul Kalam, before being elected President of India, initiated the formation of the Society for Electronic Transaction Security which later faded into oblivion. A serious adverse consequence of the inadequate state response to perceived national security threat is the emergence of private tech savvy individual hacker groups who try to counter-hack foreign websites known to be inimical to national interests. In the overall national security interest, the setting up of an apex body at the highest level needs to be pursued by the government in power.

The possibility of cyber warfare should be treated as seriously as the threat of a missile strike; the prospect of a full-blown Internet war cannot be dismissed as science fiction any more. Increased reliance on computers and management makes any nation vulnerable to cyber attacks. The only answer to the burgeoning problem lies in preparedness and vigilance. Priorities in the protection of cyber space must be clearly defined to ensure proper coordination of work assigned to various organisations engaged in this vital aspect of national security. Urgent strategic planning and institutional mechanism on a national scale is required to pre-empt any major setback in the war to secure cyber space—assuming that has not already occurred. ■

Today's Modern Battlefield

By **Valerio Monforti,**
International Sales – Area Manager,
Elettronica S.p.A.

Today's fast-moving modern battlefield is posing a serious challenge to the defensive capabilities of one's own deployed ground forces. Therefore, effective defensive assets should be widely employed in order to anticipate and prevent any unexpected attack maneuvers.

The electromagnetic spectrum plays a decisive role in these scenarios, Electronic Warfare systems constitute a mandatory capability and their operational employment requires planning and implementation of appropriate procedures.

Defensive operations relying on modern tactical EW systems with primary purpose of neutralizing opponent's offensive tactics and consenting a timely retaliatory action.

Field commanders rely on availability of real-time operational picture on enemy force deployment/tactics.

Sources of such time-critical information include:

- Geographic location of their own units
- Human-Intelligence
- Image-Intelligence
- Communication-Intelligence
- Electronic-Intelligence (ELINT)

The collected information provides such indications as:

- Deployed enemy forces
- Their capabilities
- Enemy objectives
- Direction of attack and main offensive enemy effort
- Enemy units's positions

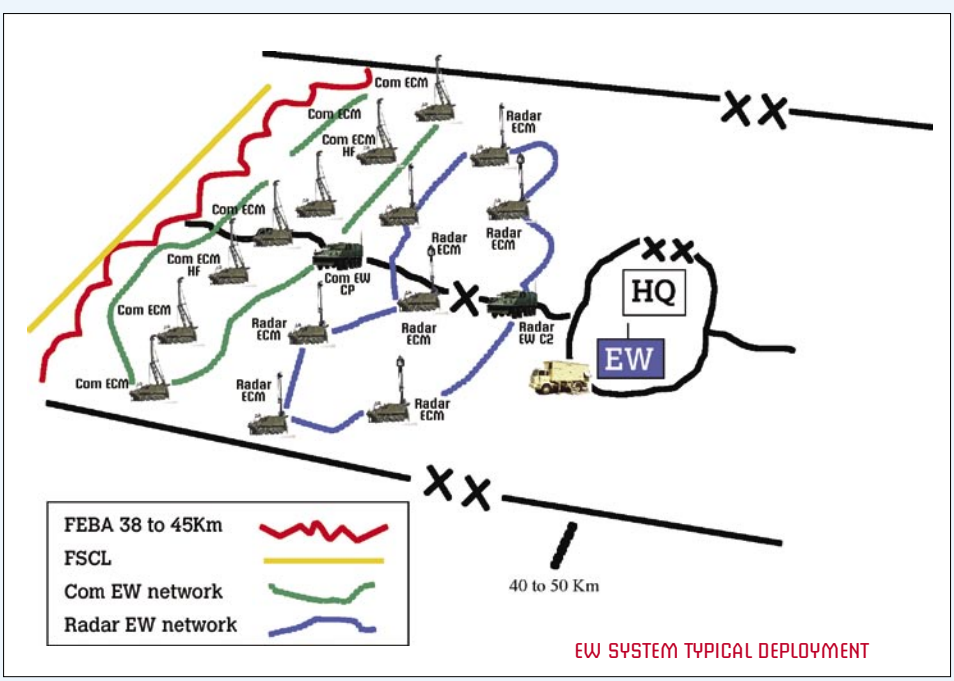
EW surveillance provides significant contribution for interception location tracking of priority emitters and their characterization, identification classification of the emitter-associated threats.

In the scenario, EW jamming plays an important role by denying the enemy's effective use of its Command & Communications systems. It prevents the enemy from properly managing its forces, exploiting its own SIGINT and IMINT data acquisition equipment, and denies targeting of friendly assets and ensures protection of access routes/operation areas to friendly attack forces.

EW SYSTEM CONFIGURATION AND FUNCTIONS:

- Analysis of EW awareness reports
- Correlation of data from other sources
- Correlation with intelligence from national data-base.
- Generate and display situation assessments
- Reports to HQ
- Definition of possible enemy actions
- Definition of own action lines
- Planning execution of orders/tasks

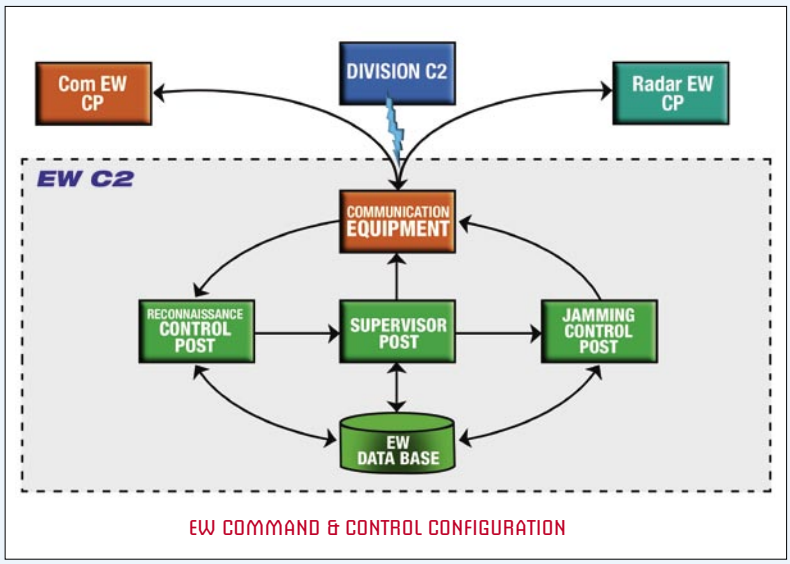
One of the key elements in the above scenario is the **Ground Radar Jammer**.



EW SYSTEM TYPICAL DEPLOYMENT

ELT/333 Radar ECM System represents one of Elettronica's latest equipment, incorporating DRFM (Digital RF Memory) and

SSAPA (Solid-State Active Phased Array) capable of ensuring a real simultaneous multi-threat capability based on advanced power



EW COMMAND & CONTROL CONFIGURATION

management techniques.

The system's unique performance combines smart and tailored jamming programs, together with high ERP (Effective Radiated Power), to generate coherent and non-coherent jamming techniques; generation of credible false targets alongside the real ones. This approach avoids the use of power-consuming noise jamming over extended frequency bands to cope with RF agility that is ineffective in terms of J/S ratio.

The equipment techniques generator exploits a multi-bit-DRFM to store the sampled incoming signal and reproduce it according to a programmed modulation.

Main features of ELT/333 are:

- Automatic Search and detection of emissions designated by the ESM;
- Parameter measurements of detected emissions ;
- Automatic response
- Interface with Data-Link;
- Capability to operate in "stand-alone mode" using its own library

Moreover, exploiting the receive/ transmit capability of SSAPA antenna, additional system features include:

- Accurate DOA measurement of single emitters for emitter-localization in "networked-operation"

The ELT/333 ECM consists of:

- Jamming Antenna Unit: performs emitters interception and jamming signal transmission.
- Monopulse Receiver: performs threat signal search and D/F processing
- Jamming Source Unit: contains DRFM and Processor and is the ECM system core unit.

JSU and the Monopulse Receiver are tasked with the search and detailed analysis of the received signals, and generate complete and effective jamming techniques/programs tailored to the threats, as well as simultaneous jamming in different Directions of Arrival.

This ECM system is based on two innovative technologies: DRFM and SSAPA Antenna.

DRFM: ensures a real multithread capability through high speed sampling of RF-signals and storing samples in large digital memories and provide a high-fidelity replica of threat signal capable of deceiving the victim radar's signal processing equipment

SSAPA ANTENNA: basic characteristic is that it can change the angular direction of its radiation pattern without any mechanical movement.

Consists of:

- ***Array of wide-band radiators*** This type of radiating element is the most suitable element for wide angular coverage array architecture operating in wide bandwidth
- ***Network of transmit/receive (T/R) modules*** producing the output power. This component is a dual-channel module in which DRFM jamming signal is conveyed along the transmit path for threat response, while the incoming signal is conveyed along the receive channel for subsequent processing and beam steering purposes.
- ***Beam-forming network*** Consisting of power dividers/combiners feeding the T/R modules and generating signals for the D/F Receiver and the DRFM.

CONCLUSIONS

The above analysis of the Radar ECM operational tasks, based on a realistic operational scenario, has yielded the following main requirements:

- jamming in emitter designated mode
- emitter designation by networked ESMs
- emitter acquisition on the basis of ESM-designated parameters using narrow scanning beam
- emitter jamming on the basis of programmed library
- jamming in stand-alone mode
- emitter search and acquisition
- emitter identification
- emitter fine DF
- emitter jamming on the basis of programmed library

The ELT/333 Radar ECM system has been specifically designed to meet such needs and its architecture combines wide-band DRFM and SSAPA to ensure:

- high ERP without duty-cycle limitation;
- low power Rx/Tx modules
- high radiated power against pulse and CW threats
- high sensitivity and emitter fine DF using narrowscanning beam;
- coherent jamming
- multi-threat capability
- emitter-acquisition on the basis of ESM-designated parameters using narrow scanning beam ■

PARADIGM Shifts

The shift from 'Industry Supplied Complete C4ISR System Procurement' to a 'Design having an industrial build' introduces fresh complexities in product development and lifecycle support

By **Captain (Retd) T.N. Pranesha, Bangalore**

The C4ISR product line has evolved over the past three decades as a prominent force multiplier. The speed of developments in the related technology domains render very high rate of obsolescence and also extreme difficulties in coping up with life cycle support associated with the deployed products. Qualitatively, the technology focus in these product lines has undergone shifts from 'Hardware Centric' to 'Software Centric' to 'System Centric' to 'Network Centric' paradigms over a period.

Invariably, doctrines drive the available technology at any given juncture to create war assets. Technology provides means for development/acquisition of war assets that provide specific capabilities to a force to achieve the goals of perceived threat neutralisation through the use of 'doctrines' and plans. Although, the military enterprises are built with the basic assumption that 'the doctrines drive the technology' there are several instances in the history where specific sets of innovations in technology creates profound impact on the doctrines resulting in an inescapable need for rapid re-evaluation and redefinition of doctrines. These are known as disruptive technologies that create paradigm shifts in the way the business of conduct of warfare is done. Advent of steam engines, nuclear weapons, aircraft and so on are examples of such paradigm shifts in the past. The Network Centric Warfare (NCW) technology is one such disruptive technology that calls for significant levels of adaptations and re-adjustments to the war enterprise.

The core technological backdrop for Network Centric warfare systems is an offshoot of the grand convergence among the computers, communication and control engineering disciplines, generally known as '3C' convergence. This convergence has resulted in demand for high performance embedded computing and increase in order of complexity of embedded software, which in turn, require leveraging diverse developments in related technology fields. At functional level, application-specific solutions are needed in embedded areas, such as sensor specific signal/data processing, Mission/operator related asynchronous event handling, distributed support for 'Peeking' and 'Poking' the contextual sensor data at decision making levels-add on to the system complexity. Further, there are new challenges for embedded systems, such as time-to-market, cost, code size, weight, power, and real-time behavior. The shift in paradigm from 'Industry Supplied Complete C4ISR System Procurement' to a 'Design having an industrial build' introduces fresh complexities in product development and lifecycle support.

A proper architectural design that embodies the concerns from diverse domains and assure paths to address the issues and problems in a flexible way over the lifecycle of the product would be an essential and inescapable prerequisite in this context. The primary objective of this paper is to give a glimpse of multiple technology areas that have bearing on the C4ISR product architecture that forms the backbone of NCW capability. An approach for moving forward in transformation of forces with transition strategies, in this context is also suggested.

EMERGING DIGITAL BATTLEFIELD

Battle command hasn't changed over a period. Commanders and leaders are still:

- Seeking Information
- Making Plans
- Executing Decisions
- Communicating
- Assessing Operations
- Changing Plans

What has changed is:

- Applying Technology
- Executing Activities with technology
- Collaborating
- Training

The capabilities that make up Battle Command have endured the test of time. The characteristics of a Net-Centric Information Space are:

- Content is:
  - Persistent
  - Visible
  - Authoritative

  - Extensible
  - Reusable
  - Interoperable across platforms
- Content supports:
  - Dynamic relationships
  - Value adding

C4ISR systems built around net-centric architecture provide core capabilities that support the battle field information needs that are shown in the figure above to the commanders at different hierarchical levels of the C2 structure of the composite force.

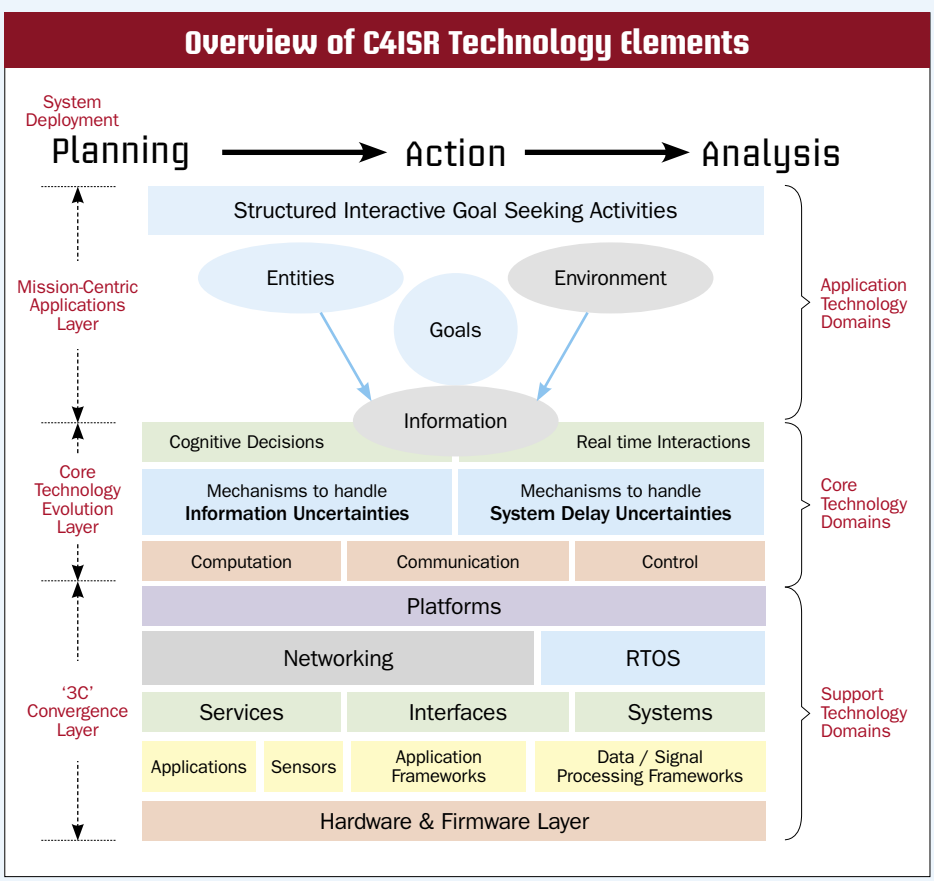
Systems based on such architecture provides robust and consistent infrastructure for exercising flexible and dynamic command and control in a hierarchical C2W structure. The qualitative differences that are incidental to the Net-centric C4ISR system is as follows:

- Information flow across the Battle Field Hierarchy is almost instantaneous
- Contextual processing and rendering of information at all levels to facilitate hierarchical role-based decision making
- Flexibility in rapid Integration and segmentation of forces based on tactical requirements
- Information flow, decision making, command and control and physical level actions in terms of battle field manoeuvres and engagements are linked entities and optimisation and alignment of the same to achieve force effectiveness is one of the objectives of capability building efforts. It may be seen that whereas, net-centric technology brings in very significant and profound acceleration to the first three entities (Information Flow, Decision Making and Command and Control functions) it has very little impact on the physical level actions. Catering for this factor in doctrine and procedures readjustments may be a challenge in transition to net-centric paradigm.
- The orders of magnitude acceleration in information flow and information processing achievable through net-centric systems coupled with the constraints that exist on physical level battlefield activities leads to the relevance of 'Non Zero Sum' game models to the war game instead of traditional 'Zero Sum' game models. This leads to a very high intrinsic potential for significant changes in doctrines as well as standard operating procedures (SOPs)
- Traditional approaches adapted for system performance evaluation prior to their induction to the service becomes irrelevant due to the difficulties involved in creation of realistic and relevant test conditions on one hand and need for identifying proper 'measures of performance' and procedures to establish the 'measures of effectiveness' in the system deployment context

EVOLUTION OF TECHNOLOGY

Developments and maturity levels achieved in the Information Technology domain has immense influence on bringing in qualitative changes in the electronic battle space. The all-pervasive ingress of IT elements in several critical, often inter-related domains, of enterprise operations is undeniable. Integration of the computation world with the physical world and connecting human players with a pervasive web of interactive computers and physical devices to create an all-pervasive, ubiquitous digital battlefield that gives decisive advantage in the conduct of warfare is the prevailing trend.

While technology evolution trends helps immensely in achieving goals of consolidation and integration of information resources that contribute to the operational success, it also opens up new



flanks of vulnerabilities in the form of tactical C2W (Command and tControl Warfare). The strategy to build infrastructure and systems in this context is to integrate information systems and devices into architectural spaces, allowing users to interact with their surroundings in an intuitive and role based manner. In light of this strategy architectural space can be considered as an interface between people and digital information. This is essentially leading the equipment and system design trends to the concepts of 'Mission Centric Networks', 'Network Centric Combat Systems', 'COT's based Systems and Sub-systems', 'Middleware Centric System/ Sub –system Integration' and 'Open Standards based Intra/Inter System Connectivity' paradigms. The above brings in the following additional issues at C4ISR system design context:

- Need to determine the criteria for communication system automation that ensures communication system improvements in terms of:
  - Rapid, reliable, and re-configurable communication systems
  - Transparency of Communications to the Battle staff
  - Increased Communications capability with reduced operator Manning
  - Real time indication of Fault
  - Provisions for graceful Communication system Degradation.
- Seamless, reliable communication systems and services will more effectively enhance and support Command and Control (C2) requirements now and into the future. Superior communications is achieved through the implementation of:
  - Seamless connectivity among strategic and general forces
  - Integration of tactically significant information into ashore, afloat, and in the air assets
  - Identification of communication systems and functions that will benefit from automation
  - Ensure automated C2 Assistance for command Decision makers

C4ISR & NCW

With widespread availability of digital broad band access technologies at intra system interconnection and ship system infrastructure levels, coupled with robust digital communication links at ship-to-ship, ship-to-air and ship- to-shore levels the design choices at product architectural level are very high. Further, the maturity and availability of very high performance heterogeneous processing platforms (Multiple RISC + DSP + Network Processors on common silicon substrate), integrated tool chains and development environments and third party resources for technology and application domain specific middleware for the selected platforms lead to further level of choices in architectural design space. It is appreciated that the enormous market potential coupled with the diverse application needs associated with networked distributed applications segment would bring in a paradigm shift in product development approach for the next generation network centric products and systems like C4ISR.The main features of this shift are:

- Shift of product design focus from current hardware centric/software centric approach to System Centric/Network Centric approach
- Differentiation between the 'Combat Systems QR' and 'Combat System Specifications' and approaches for bridging the gap between the two are important for the system acceptance and success in this context.
- A clear understanding and addressing of the 'Functional (Desired)' and the 'Incidental (Undesired)' performance issues assume key importance in achieving smooth system induction
- Evolvable Solutions and Products that enable Transition and phased update of Technology and Functional Features
- Emphasis on reusable software and flexible, re-configurable hardware platforms. Easy scalability of solutions
- Understanding and addressing of what is necessary to generate demand for technologies that have the 'potential to re-structure missions and warfare' or for technologies that meet inchoate needs and have potential to create new missions and forms of warfare is essential in this context.
- Development of diverse customised solutions using standardised hardware, reusable middleware and Software building blocks resulting in 'economy of scope' rather than 'economy of scale' as an index for technology and market competitive advantage for the building blocks as well as end products.
- Further, the recent shift of focus in major research efforts associated with the large high performance networking technology from traditional defence driven programmes to market driven programmes centered around academic institutions have rendered open access to the technology.

APPROACH TO CHALLENGES

The transition requires creation of a suitable product architectural framework based on a reference model for C4I2SR (Command, Control, Communication and Computer systems for Information and Intelligence Surveillance and Reconnaissance) and phased migration of the existing applications with essential technology updates to the new architecture. The approach outlines the adaptation of a distributed objects technology-based middleware, like Real time CORBA and DDS (OMG standard for Data Distribution Service for Real Time Systems), as an application integration framework, supported with IP Core network for transportation and a variety of access networks that connect sensors and other resource clusters to the network.

Support for several newer equipment/modules as functional building blocks of the system in the form of sensor specific raw data compression and decompression units, local data fusion units (that fuses multi-sensor situational picture along with contextual raw data for global delivery), global data fusion units with decision support capability, node level security policy enforcement modules and Tactical IW surveillance and attack systems as an integral part of the futuristic C4ISR paves way for building a formidable force multiplier to support future warfare.

The key concept is to establish a path of evolutionary shift in the existing/evolving product that enables phased update of technology features and the approach to the conduct of warfare with short turn around times and with full protection on investments made on legacy systems, at each stage inclusive of the life cycle support for C4ISR and NCW systems. ■

Conceptual Underpinnings

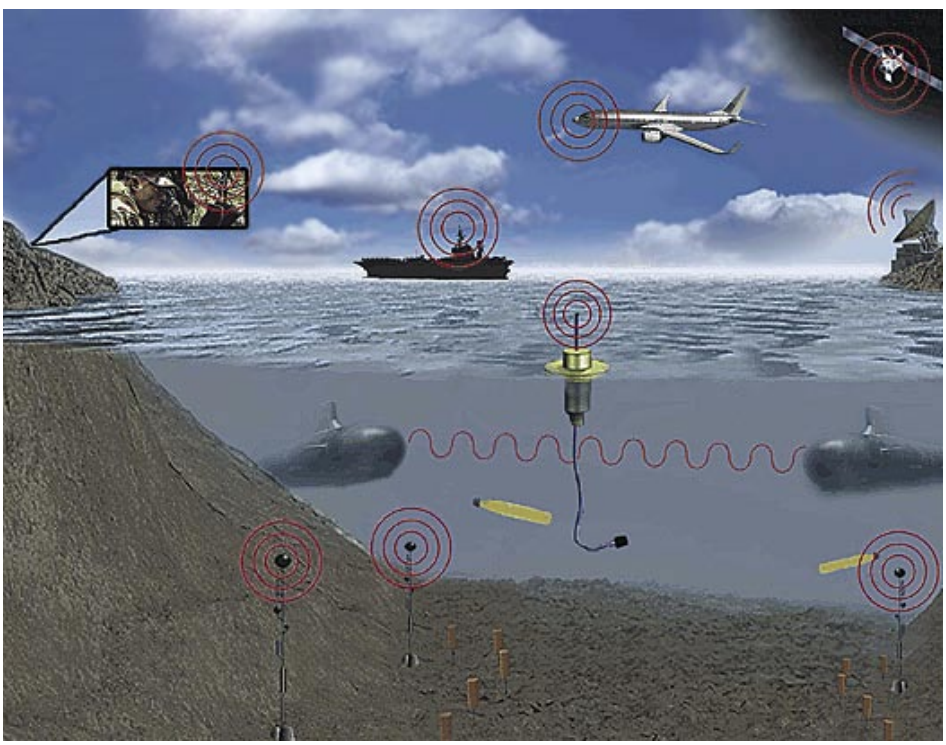


ILLUSTRATION: WWW.NAVY.MIL

Service-based C4ISR solutions for net-centric defence have several distinct benefits that enhance and improve operational capabilities

By **Commander Devbrat Chakraborty**

The value chain in a network centric environment comprises of several layered concepts:

- **Data Quality** is at the most fundamental level and describes the information within the underlying command and control systems.
- **Information Quality** indicates the completeness, correctness, currency, consistency, and precision of the data items and information statements available.
- **Knowledge Quality** deals with procedural knowledge and information embedded in the command and control system such as templates for adversaries, assumptions about entities such as ranges and weapons, and doctrinal assumptions, often coded as rules. In the more evolved systems, this component would comprise more and more of modeling and simulation systems. Knowledge quality is the first component related to the common model of the operation.
- **Awareness Quality** measures the ability to use the infor-

mation and knowledge embedded within the command and control system. Awareness lies in the cognitive domain that is at a level that is above the level of technical interoperability.

Efficient conduct of operations is enabled by the ability to share data, information, knowledge and awareness. In other words, the IT value chain accompanies the network-centric value chain. More importantly, this is reflected in improvements in command, control, communications, computers, information, surveillance and reconnaissance (C4ISR) over the recent decades. C4ISR systems initially started as database centric and message driven solutions, only able to support Data Quality. To progress to the next level within the value chain, the idea of the Common Operational Picture (COP) was introduced, thereby adding context to the data. The COP, thus, improved not only Data Quality, but also Information Quality.

Modelling and simulation abilities in a C4ISR system add procedural knowledge in the form of models. Such a system can thus support the next level in the value chain, triggering further improvements. Evolving further, the ability to use this information, as distinct from understanding it, is aided by the system's ability to mine, analyse and present data for decision support and this is pertinent in the Awareness Quality context. The underlying fact of course is that it is far more necessary to bridge the cultural gaps rather than the technical gaps to make this vision become reality. Interoperability aspects of networks come to fore, if robust defences are to be built in.

NetcentricValue Chain Layer	C4ISR Solutions and Offerings
Data	Data Base Centric, Message Driven
Information	Common Operating Picture
Knowledge	Modelling and Simulation
Awareness	Analysis and Decision Support

In addition to Situation Adaptation, Interoperability and Open Standards, salient features and indeed principles of C4ISR Systems in a network-centric environment are discussed in detail below.

SERVICE ORIENTED ARCHITECTURE

Increasingly, C4ISR solutions for network-oriented defence are based on a Service-Oriented Architecture (SOA) where the functionality of a system is made available as services that can be accessed by any authorised user connected to the network, mobile or stationary. This makes it possible to avoid large "stovepipe" systems, designed only for a specific purpose, and instead make it possible to combine individual systems into systems-of-systems. Even geographically distributed systems can then be used as modular building blocks that are interconnected and can be combined in different ways. The two key categories are Services and Infrastructure. Services pertain to services for Communication and Collaboration, Situation Information, Information Operations, Command and Control and Engagement Support. Infrastructure includes a Control Layer, a Convergence Layer and a Connectivity Layer.

The Communication and Collaboration services provide functionality for communication and information sharing. Situation Information services involve gathering, processing and dissemination of situation information. Information Operations include services for assessment and influence on other parties' situation information and also for protection of the own situation information. Command & Control involves services for decision support and order handling. Engagement systems and effectors are connected to the C4ISR environment and are involved in the information flow and controlled by Engagement Support services. The Control Layer contains functionality and support services that are used to give all the services mentioned above the required characteristics and features such as security, mobility, and accessibility. The Convergence Layer ensures that connectivity can be accomplished in a unified manner based on the Internet Protocol (IP) and different types of fixed and wireless networks, belonging to the Connectivity Layer can be used.

DISTRIBUTED SYSTEM-OF-SYSTEMS

The C4ISR system is to be regarded as a distributed system-of-systems with each system producing and/or consuming services. The producers and consumers of various functions are separated. Thus, services are not necessarily produced for a single particular purpose and their production is independent of the consumers. These are available for any authorised consumer to use. This also means that services and information reside in the system as a whole, integrated and aggregated, thereby creating services and information with a higher value.

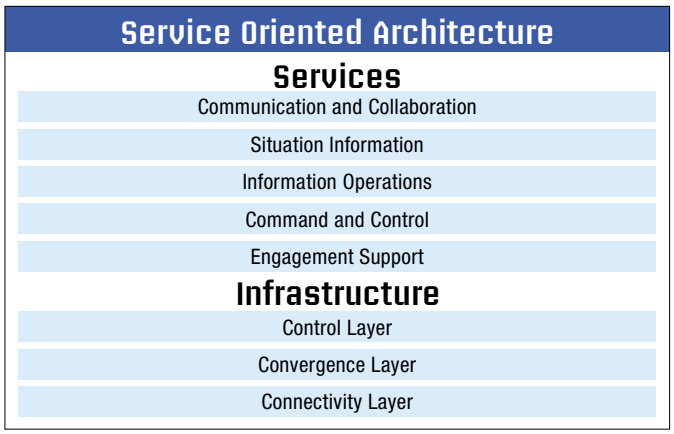
Further, infrastructure and/or technical systems producing the services need not be new and existing legacy systems can be integrated. Finally, systems are scalable and hence services and capabilities can be further developed in an evolutionary fashion.

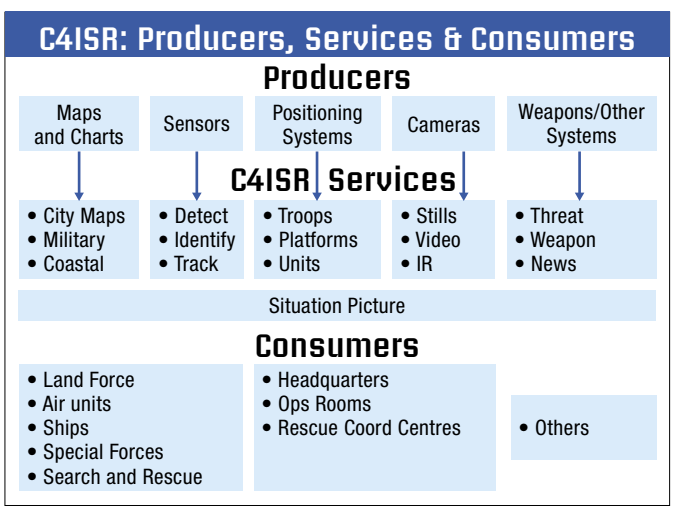
COMMUNICATION NETWORK

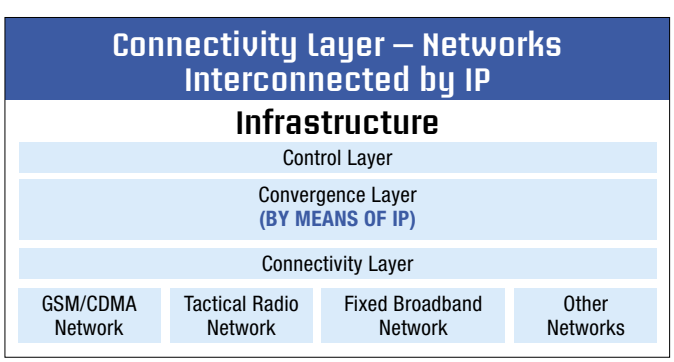
In keeping with the system-of-systems approach, the best, and often the most practical option, is a network-of-networks, utilising a variety of communication technologies. These are also called heterogeneous communication networks. Communication networks may have different origins: public, private, defence, governmental and so on, and may include tactical radio, broadband networks, fixed telephony, and mobile networks. The trick is to use the IP as the common communication protocol.

Dedicated non-IP networks may, however, be necessary in situation and applications where real-time information is critical. The network-of-networks approach puts special requirements on infrastructure functionality, like routing, addressing, mobility, quality of service and security. These can be based on commercially available technologies with additional security, robustness, and flexibility requirements as deemed necessary; as they can be cost efficient and make use of the most advanced components and technologies available. For example, GSM and CDMA based systems can be used in many applications. The main advantages of the network-of-networks approach are:

- Improved efficiency and a reduction of equipment and operational costs. Ability to dynamically compose networks depending upon where network resources are needed for the moment.
- Much higher redundancy since even if one equipment is damaged, others continue to operate and joint communications are maintained using alternative paths. Even if all inter-network connections are lost, sub-networks are formed that can later be reconnected.







COUNTING THE BENEFITS

Situation Information: Adopting the concepts described above results in trustworthy and recognised situation pictures, potentially shared in near real time leading to an understanding of the overall situation. This also enables access to key information for different types of actions, and improves generation of corroborated information from complementary sensors—such as radar, electro-optics, and signal intelligence sensors—and other sources. Also, surveillance operations can be managed to continually optimise sensor resources.

For instance, in a situation with a temporary threat or a specific planned activity there may be a need to move mobile platforms to preferable geographical locations, tune the sensor usage, or to add supplementary sensor resources. All this fundamentally changes the capability to achieve situation information to an entirely new level:

- Information is derived from a substantially increased number of sources of different kinds: sensors, intelligence, databases, collaborating authorities and organisations, and other external sources such as news, media, weather forecasts, websites and so on.
- Efficient processing and fusion of information leads to situation information that is accurate and has low levels of ambiguities.
- Role-based situation pictures, that is, excerpts of the situation information, can be accessed by any authorised user anywhere and anytime.

Information Operations: Information operations involves intelligence, influencing and suppressing the opponent's situation information, protecting the own situation information, and managing the information flow to external parties. Intelligence capabilities are improved in much the same way as the capability to achieve situation information. A large number of sources can be managed and high-performance communication services can be widely and readily accessed with the requisite degree of security even when using the public communication infrastructure. Sharing of information among various decision makers facilitates synchronised planning and conduct of operations. In particular, improved coordination between organisational levels can be achieved. This further leads to shorter decision cycles. Other essential factors that improve decision quality are the ubiquitous access to advanced support services like:

- Resource optimisation
- Decision support
- Simulation including evaluation of possible action alternatives.

Engagement Support: When so connected, the entire range of command and control systems, effectors, and information resources are made available for the engagement functions. For example, situation adapted sensor-to-weapon loops that utilise the optimal combination of information sources, command and control functions, and engagement platforms can be established

IN CONCLUSION

Service-based C4ISR solutions for net-centric defence strategy have several distinct benefits that enhance and improve operational capabilities, such as flexibility, cost efficiency, evolutionary growth, interoperability, robustness, connectivity and security. The services on the net approach gives the possibility to interconnect and utilise new and existing systems in a cost efficient way.

Commercially available technology can be utilised whenever it meets requirements. C4ISR solutions can be adapted to different situations, thus allowing units to operate across organisational as well as technological borders. Further, such solutions lead to cost efficiency and allow distribution of desired information and functionality to anyone authorised, anytime, anywhere in the network of networks. ■

The writer is a Research Fellow, National Maritime Foundation.

PHOTOGRAPHS: SP GUIDE PUBNS

E-SPY: The IAF's AWACS is equipped with Phalcon radar on an IL-76 platform

Fill in the GAPS

A networked AD environment would be rich in wireless signal traffic and thus vulnerable to interference. So data links have to be robustly protected—both against eavesdropping and jamming.

By **Air Marshal (Retd) A.K. Trikha, Pune**

In the history of organised armed conflict, vesting command and control of assigned forces with a designated commander for achievement of a specific mission has been a fundamental feature since times immemorial. In executing his executive 'command and control' functions, the commander relies on information or intelligence from a variety of sources. Timeliness, quality and noiseless intelligence being crucial to commander's quality of decisions, the 'I' (for intelligence) gets closely tied with the C2 functions. Communications being the conduit through which information or intelligence is exchanged, the co-efficient of their effectiveness gets directly linked to the C2I function, which expands the equation to C3I. The vast amount of data generated on a modern battlefield can neither be collated, analysed, synthesised nor disseminated, (to generate actionable intelligence) without adequate data processing support being integrated in all component parts of the system. Computers have, therefore, become ubiquitous enough for another C to merit an equal status in the C3I paradigm. C4I, thus, represents an integrated architecture in which the quality and effectiveness of a Commander's executive 'command and control' function gets directly linked with the comprehensiveness and quality of Intelligence obtained and disseminated through a variety of communication channels, and how each aspect is supported and enhanced by different degrees of automation provided by computers. The sum total of support element in the C4I build is to sift, sort, integrate and present all relevant information in an easily digestible format in real time so as to enable decision makers at all levels to be completely aware of the 'situation'.

Different militaries have added letters to this basic acronym (C4I) to create an alphabet soup corresponding to their understanding of grouping of military functions which assist the 'command and control' process. Thus, the British have added a STAR to C4I, to indicate inclusion of 'Surveillance, Target Acquisition and Reconnaissance' as significant components. The US military calls it C4ISR to bring Surveillance and Reconnaissance under the same tent. There are many more variations to this general theme of support elements or aspects related and tied to 'command and control'.

WAR-FIGHTING & C4I

Quantification of C4I components and their individual contribution to combat effectiveness is abstract. However, their correlation with a well-known and well-understood combat process makes the significance clear. As in any predator-prey interaction, every military engagement goes through a process of observation, orientation (that is, of putting what is observed in its appropriate environmental context), an iterative process of decision making before initiation of action or an appropriate response—as described by John Boyd in his OODA (Observation, Orientation, Decision, Action) loop.

Observation, orientation and decision making are information centric; in other words, they are about collection of information, its interpretation, contextualisation and dissemination—based on which decisions are made at various levels of command. Robust communications, automatic or computer assisted processing of intelligence data gathered through a variety of sensors, as well as in decision making, as encapsulated in the C4I para-

ONE FOR THE ALBUM: India's first AWACS was inducted into the IAF on May 26

digm, have a direct bearing on the OOD aspects of the OODA loop. The faster information can be gathered, collated, analysed and disseminated, the faster and more appropriate the response would be. The secret of success in an engagement at any level lies in outpacing the adversary in the OODA loop, thereby imposing upon him an operational tempo with which he cannot cope.

C4I IN THE IAF

Peace or war, air defence (AD) should never sleep. It is a 24x7 engagement. Existence of vast gaps in the radar coverage of Indian air space even at medium level is a well known fact. At low level, the Indian Air Force (IAF) has been making do with a handful of indigenous Indra 1 and 2, Russian ST-68s, and some P-18 low level surveillance radars detached from the SAM units. In times of tension, they move forward from their home locations to watch a narrow band of territory along the International border.

Even in this narrow, linear belt, gaps remain—both due to paucity of numbers as well as difficulty of deployment in the very challenging environment. Networking is minimal and relies solely on voice communication. The quality of communications is even less flattering. Legacy HF and cumbersome mobile troposcatter VHF systems constitute the backbone for surface-to-surface communications. The system has never really been put to test in an operational scenario, but the crippling shortcomings are obvious. The IAF is currently in a phase of rapid transformation.

AEROSTAT RADARS: In 2006, the IAF started deploying EL/M-2083 tethered Aerostat Radar Systems imported from Israel. Two have already been deployed, one in the Kutch region of Gujarat and the other in Punjab. While four more are reported to be in the pipeline, the total IAF requirement is said to be for 13 such systems. Elta Systems EL/M 2083 Aerostat Programmable Radar (APR) is derived from the company's L-band (1 to 2 GHz) EL/L-2080 'Green Pine' ground-based, phased-array radar used in conjunction with the Arrow missile defence system. It is a 3-D sensor that can track and illuminate targets travelling at velocities in excess of 3,000 m/s. Therefore, in addition to aircraft, it can also track such targets as cruise missiles, unmanned aerial vehicles (UAVs) and microlights.

AWACS: In May, the IAF received its first Airborne Warning and Control System (AWACS) aircraft from Israel. Built with Phalcon radar on an IL-76 platform, it is said to be one of the world's most advanced systems. The phased array radar (which does away with the need for a mechanically rotating antenna), can detect low flying aircraft, cruise missiles and UAVs hundreds of kilometres away by day and night and under all weather conditions. In addition to the radar, the aircraft also carries a phased array IFF and a host of electronic and communications, support and intelligence equipment.

OTHER AD HARDWARE: The IAF also plans to acquire a wide variety of radars and surface-to-air weapons to equip itself with a more respectable capability of AD at all altitudes. Most of these requirements are being sourced from Israel, which has emerged as India's principal supplier of high tech weaponry. The IAF also plans to put in place an Integrated Air Command and Control System by the end of 2009 which is expected to put all sensor platforms (both airborne as well as surface facilities), weapon systems (Surface-to-Air Guided Weapon System, or SAGW, batteries and fighter Aircraft) on a common grid. The year after, the IAF plans to launch a dedicated satellite. With the planned acquisition of 230 Su-30MKI air dominance fighters and 126 medium multi-role combat aircraft all networked into a comprehensive web, it looks as if the country's AD is about to witness a complete make over. However evaluation of goals vis-à-vis current status and past experience would tend to suggest cautious optimism at best. While each of the individual components—aerostats, AWACS, Low Level Transportable Radars (LLTRs), 4 and 4.5 Generation fighter aircraft, more effective SAGWs and so on—would represent a leap in capability in their own right, the single most significant component of this make-over is networking. The net increment in capability brought about by 'networking' is believed would far exceed the sum of its individual parts.

COMPLEXITIES & CHALLENGES

Speed with which digitisation and networking has swept the market may convey the impression that a similar revolution in the AD network is just a matter of putting some gizmos in place. Reality, however, is different and far more complex. In the first instance wholesale replacement of all legacy, analogue sensors with digital ones would take considerable time and money. Deployment of sufficient number of digitally networked Aerostat radars would facilitate comprehensive surveillance of vulnerable airspace. Similarly, AWACS would also dovetail into the system relatively easily. However, the Aerostat/AWACS arrangement doesn't render LLTRs redundant.

Another inconvenient truth is that securing a link against interference (encryption) as also making it reasonably jam resistant eats into its transmission channel capacity—a serious constraint when high rates of data transfers are required. To maintain sufficient rate of data flow, the links usually remain less than robustly protected. During hostilities, the front tier of radars would still be necessary to cater for non-availability of aerostat or AWACS coverage. Digitisation of the IAF's SAM-III systems ran into rough weather some years back. Whereas acquisition of some new systems appears to be in the pipe line, wholesale replacement doesn't appear feasible in the short term. Developing Interfaces for AD fighters of different vintages and pedigrees to communicate with the network is also not likely to be easy. In a nutshell, our perfect networked future may still be quite distant. ■

Information Integration

The ability to collect, process and disseminate flow of information, leading to increased mission space awareness and subsequent dominance, constitutes the essence of present day air operations

By **Air Marshal (Retd) V.K. Bhatia**

Ability to collect, process and disseminate flow of information leading to increased mission space awareness and subsequent dominance constitutes the essence of present day air operations, firmly fixed in a classical extended C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) framework. The latest buzzword is to also include 'Target Acquisition' to complete the sensor-shooter loop. Success of such operations is ensured through shared situational awareness, close collaboration, co-ordination of capabilities, and the ability to react quickly to highly dynamic modern airborne threats.

Networking of widely dispersed ground-based sensors (radars, visual observation posts, passive electro-optical and RF sensors), multi-spectral sensors on a host of airborne platforms (combat aircraft, Airborne Warning and Control System, or AWACS, Unmanned Aerial Vehicles, or UAVs, aerostats, and so on) and processing of massive data flow from such diverse sources to generate a comprehensive air picture in a defined air volume is first and, by far, the most important sub-set of air defence (AD) operations. The air scenario—referred to as operational situation picture (OSP) or air situation picture or recognised air picture—has to be both comprehensive and stable to serve as the main source of information for decision making at various echelons of the command structure. Since the quality of decisions that emanate at various levels of a networked system (in the areas of threat evaluation, force application and battle management) depends directly upon the quality of air picture, the manual or so-called semi-automatic networks are inadequate for controlling modern day air operations.

As technology continued to evolve in terms of better sensors and computing power, technologically advanced air forces the world over re-defined the roles, functions and responsibilities of the then existing conventional AD organisation and its intervening command echelons to encompass all air operations and not remain confined to AD functions alone. It was but a natural evolution. For effective AD, air space management is a precondition and, for that a total knowledge of spatial orientation of all friendly air vehicles (fighters, transport aircraft, surveillance platforms, armed helicopters, UAVs, and so on) in the given air space was mandatory. With such data being available, conduct of all air operations such as mission planning of own aircraft, storage and dissemination of target data, issue of air tasking orders to bases, control of support elements (tankers, UAVs, AWACS), tactical routing to avoid space and time conflict, search and rescue operations, and so on from a single control centre made logical sense. The AD Control Centres thus evolved in to Air Operations Control Centres, while the intermediate node, normally called the AD Direction Centre (ADDC) in the earlier structure, was either replaced by a Control and Reporting Centre (CRC) or eliminated altogether, depending upon the geographical factors and traffic density.

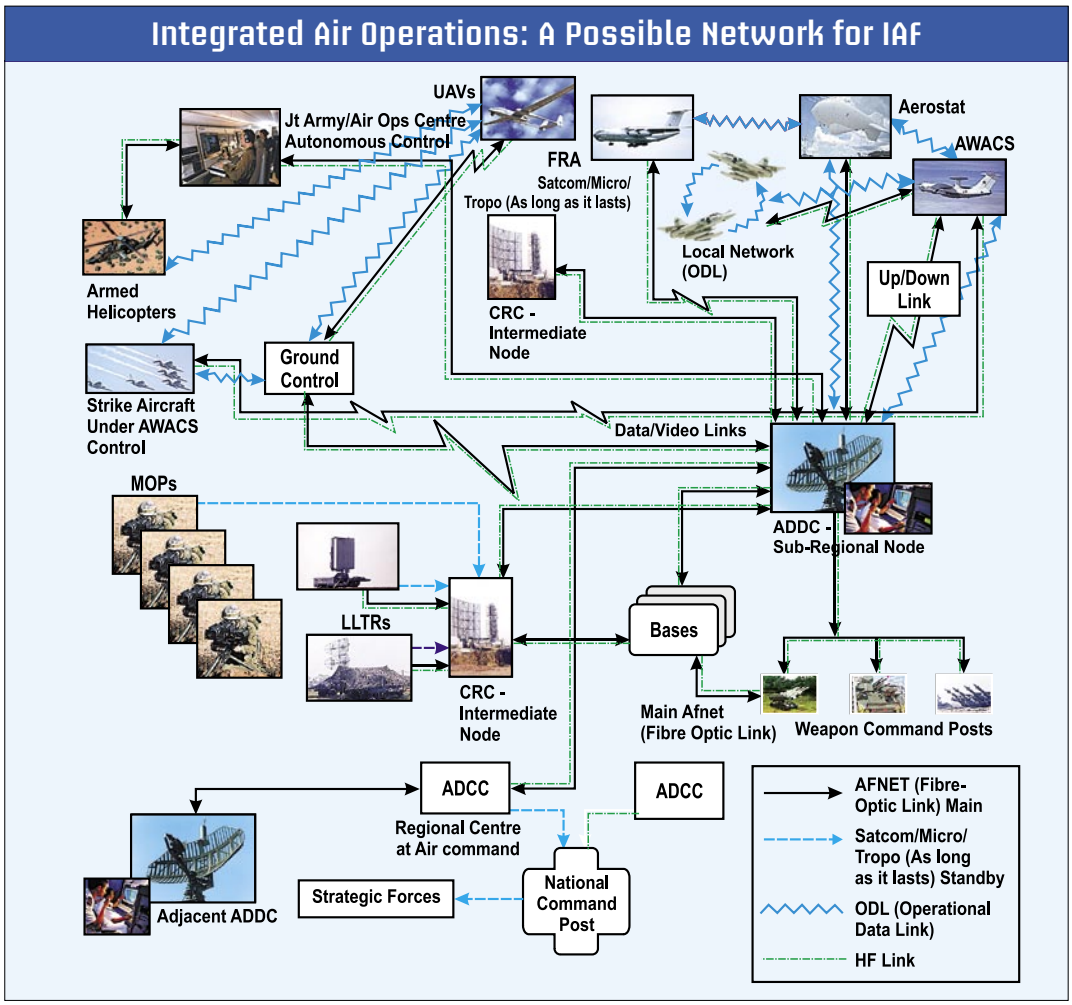
INDIAN SCENARIO

AD operations in India acquired a formal structure only after the 1962 war with China. Following the 1962 setback, new hardware and command and control (C2) structure were acquired and the doctrine defined, to establish the AD network with active assistance from the US. ADDCs, collocated with high powered Westinghouse Star Sapphire radars, were established as the nodal points for regional AD and tropo-scatter communication links engineered between major nodes. The C2 structure then established has continued to survive till date, albeit with certain modifications.

The connectivity between various nodes and echelons of the AD structure was ensured through a dedicated communication network based on tropo-scatter and line-of-sight microwave. Exchange of data and its processing, however, remained manual. The data handling and processing system was periodically upgraded with the introduction of semi-automatic data handling equipment and subsequently through an indigenously developed automatic data handling system. In the mid-1980s, the IAF also launched an ambitious project to develop an automated CRC through a Defence Research and Development Organisation (DRDO) managed organisation, called the Low Level Radar Networking Group. In the early 1990s, indigenous development of Futuristic Automatic Data Handling System (FADHS) by a public sector unit was also launched to enable better integration of assets and faster decision making.

After many years of development and considerable expenditure, both the automatic CRC and FADHS projects failed to achieve most of the design objectives, compelling the IAF to structure interim ad hoc solutions—essentially manual in content but backed by a few automatic modules for interceptions, mission planning, and so on. Subsequently, the IAF realised that given the complexity of integrating radars of varying technological vintage and capabilities,

Integrated Air Operations: A Possible Network for IAF



as well as futuristic systems like the aerostats, AWACS and modern ground-based radars that the force had proposed to acquire, it was not possible to engineer a comprehensive network, based on indigenous capability alone. Also, the network, thus structured had to have the capability to integrate all air operations under one control centre rather than remain confined to AD alone. Accordingly, the IAF proposed to acquire five Integrated Air Command & Control Centres (IACCS). Around 2003, in a major reversal of decision, the IAF re-oriented its approach by suspending the acquisition process which had reached an advanced stage and decided to develop the IACCS with indigenous effort.

DEVELOPMENT STRATEGY

Crux of a system like the IACCS lies in creating a stable OSP from the inputs of varying quality and reliability received from a host of sensors. The technique, called multi-sensor tracking (MST), requires a multi-disciplinary design support of scientists and statisticians, backed by experts in real-time systems. The OSP has to be available at all control nodes upward of the ADDC right up to the National Command Post, albeit with more data getting included at each higher rung.

The MST module has also to be supported by a host of on-line and off-line application software modules for faster decision making, air space management, optimisation of radar sites, mission planning, conflict resolution, weapon allocation, control and simulation. The system architecture also needs to have flexibility to accept sensor data from airborne platforms like the AWACS, fighter aircraft equipped with high performance long range radars (NO-11 on Su-30MKI, for example), aerostats and UAVs with Synthetic Aperture Radar payload. In addition, it should incorporate hardware and software interfaces for uploading/downloading of data and video on data links of different standards. Finally, although not part of the IACCS, to make the system operational, a strong multi-spectral communication backbone is also required.

BUILDING CAPABILITIES

At the heart of the air force's communication network is the Air Force Network (AFNET)—a dedicated IAF fibre-optics network that offers up to 500 MBPS encrypted, unjammable bandwidth. This bandwidth should be more than adequate for IAF's current and foreseeable requirements of network activity vis-à-vis air operations, including AD, UAV imagery, high-definition video streaming, and so on, besides administration and logistics.

A military satellite is expected to be launched next year, *inter alia*, to streamline the massive data flow. The recently inducted AWACS will spearhead the IAF's network-centric operations around which the other NCW elements will coalesce. Although some IAF elements have operated under the AWACS environment in some of the recently conducted joint international air exercises, in the long run, the IAF will have to devise its own AWACS strategies. Hopefully, the work has already begun with the first AWACS at its home base in Agra. Creating and maturing operational capabilities with the AWACS in the true sense of network-centric warfare will be the ultimate challenge for the IAF's leadership. ■

The Ultimate Tool

PHOTOGRAPH: WWW.INDIA-DEFENCE.COM

EYE IN THE SKY: The Indian AWACS

Having the AWACS afloat is one thing, the actual assimilation of airborne early warning and control to make combat operations lethal is quite another

By **Air Marshal (Retd) V.K. Bhatia**

Induction of the first Airborne Warning and Control System (AWACS) aircraft on May 28 heralded a major milestone in the Indian Air Force's (IAF) drive to enhance combat capabilities. One of the most crucial force-multiplier projects for the IAF, the AWACS programme was delayed by close to two agonising years before the first of the three contracted AWACS aircraft touched down on Indian soil and was deployed in the No. 50 Squadron based at Agra. According to the revised delivery schedule, the second and third aircraft are expected to be delivered by the beginning and middle of 2010.

For the uninitiated, AWACS is an airborne radar system designed basically to detect aircraft. Used at high altitudes, the radar not only allows the operators to distinguish friendly and hostile aircraft hundreds of miles away, but also to control both defensive and offensive air operations. The system is used offensively to direct fighters to their target locations, and defensively to counter enemy air attacks. It can also be used to carry out surveillance and, command and control battle management functions.

POWER OF THE PHALCON

The Indian AWACS is a unique blend of Russian hardy aerial platform IL-76 with state-of-the-art Israeli airborne Phalcon system. This has come about as a result of a tripartite deal signed in 2004 by India, Israel and Russia according to which Israel was to install the Phalcon AWACS systems (worth $1.1 billion; Rs 5,306 crore) on three Russian IL-76 aircraft ($500 million; Rs 2,410 crore) for sale to India—with the first system being delivered in 2007. The IAI/Elta Phalcon system incorporates the EL/M-2075 Active Electronically Scanned Array (AESA) phased array radar. The radar consists of array transmit/receive modules that allow a beam to be electronically steered, making a physically rotating rotodome unnecessary.

Other than the radar, the Phalcon system's sensors also include IFF, ESM/ELINT and CSM/COMINT. A unique fusion technique continuously cross-correlates data generated by all sensors: this data is combined with an automatically initiated active search by one sensor for specific targets detected by other sensors. One of the greatest advantages of the system is that radar beams can be pointed at any direction in space and time with the beams' parameters fully controlled by the radar computer. The radar employs a flexible time-space energy management technique with many additional advantages such as: selectable surveillance, optimised detection and tracking, fast track initiation without false alarms, extended detection range and, high fault tolerance and redundancy.

LINKS & INTERLINKS

Another notable feature of the Phalcon is that its advanced ESM/ELINT system is fully integrated with the radar and other sensors. Serving as one of the most important elements of the identification process, it is designed to operate in very dense signal environments, providing simultaneous 360 deg coverage. The system also collects and analyses ELINT data.

The cavernous inner fuselage of the IL-76 offers voluminous space for the AWACS aircraft to be transformed into a de facto Air Defense Direction Centre-cum-Command Operations Centre. The Indian AWACS can field up to a dozen consoles for different operators to man these simultaneously, which can cater fully to the multifarious tasks being performed continuously at the same time. Therefore, while the aircraft is engaged in passive tasks of gathering electronic and communication intelligence, it can also be actively engaged in directing air-dominance fighters to create sanitised corridors by freeing them of enemy air opposition and controlling the strike packages to proceed to their targets through the safe airspace so created.

Simultaneously, it can also carry out real-time management of the battle field within its area of coverage including directing airborne platforms for counter surface force operations—Battle Field Area Strikes and Close Air Support. The complexity of tasks entails that the entire gamut of AWACS operations be entrusted to an onboard 'Mission Controller', wielding overall responsibility, a necessity which the IAF is likely to follow. Having the AWACS afloat is one thing, the actual assimilation of airborne early warning and control to make combat operations lethal is quite another, achievement of which will be highly challenging for the air warriors of the IAF.

When fully and correctly operationalised, there can be little doubt that the AWACS can turn out to be the ultimate airborne tool in conducting network-centric air operations. ■

ALERT to danger

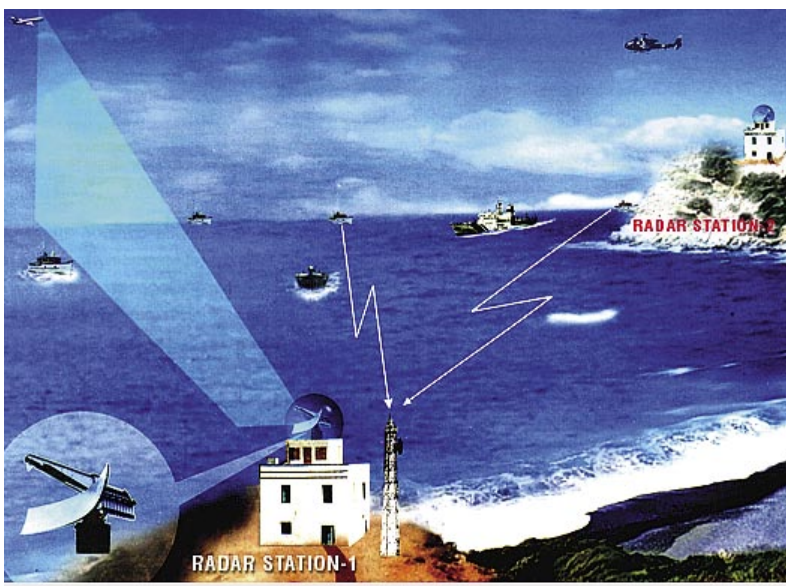


ILLUSTRATION: WWW.GIDITEK.COM

24x7

To 'see first, understand first, act first, and finish decisively' in support of homeland security operations, a seamless C4ISR system is required

By **Lt General (Retd) Naresh Chand**

Terrorism depends on surprise in terms of selection of time and place as the maximum damage can be carried on a target which is not prepared. With effective actionable intelligence, terrorists can be preempted and damage reduced or prevented. Thus, an effective intelligence and warning system is an essential component of any effective homeland security system to preempt, prevent and if necessary allow proactive action. The National Strategy for Homeland Security of the US identifies many initiatives in this area:

- Enhance the analytic capabilities of the FBI
- Utilise dual-use analysis to prevent attacks
- Create 'smart borders'
- Increase the security of international shipping containers
- Recapitalise the US Coast Guard
- Track foreign terrorists and bring them to justice
- Prevent terrorist use of nuclear weapons through better sensors and procedures
- Detect chemical and biological materials and attacks
- Improve chemical sensors and decontamination techniques
- Develop systems for detecting hostile intent
- Apply biometric technology to identification devices

INFORMATION SHARING & SYSTEMS

Information systems contribute to every aspect of homeland security and thus there is a need to design their architecture accordingly. Databases used by all agencies should be interconnected to enable sharing. The communication system should be interoperable and capable of handling vast amount of voice, data, images and documents in real-time/near real-time. The National Strategy for Homeland Security has identified five major initiatives in this area:

- Integrate information sharing across the federal government.
- Integrate information sharing across state and local governments, private industry and citizens.
- Adopt common 'meta-data' standards for electronic information relevant to homeland security.
- Improve public safety emergency communications.
- Ensure reliable public health information.

At present, 58 state fusion centres are operating 24x7 to integrate data received from state police, local security agencies and National Counter Terrorist Centre (which itself receives and integrates data from 16 intelligence communities). Some other aspects are:

- The system must react like the military in terms of absorbing situational awareness, understanding the situation and then acting rapidly.
- Coordination of even local agencies is difficult due to overlapping responsibilities and jurisdiction. It becomes even more complex if national agencies are also involved

due to separate SOP's, equipment, interoperability problems and jurisdiction.

- ISR part of the C4ISR collects, collates and analyses information about an incident. It then presents it as a common operating picture (COP) to the decision makers. Use of multiple sensors and fusion of sensor data can alert various responders. The challenge is to fuse the data in one common picture but be cautious enough about information overlap.
- Some agencies in the US use the term Network Centric Warfare for the military and Network Centric Operations (NCO) for homeland security. One definition of NCO is, 'participating as a part of a continuously-evolving, complex community of people, devices, information and services interconnected by a communications network to achieve optimal benefit of resources and better synchronisation of events and their consequences'. It is, thus, clear that there are very good civilian applications of NCO for homeland security.

C4ISR EXPLAINED

The US office of Homeland Security has extensively studied various C4ISR models which could be used for homeland security. After an extensive study it was concluded that the network architecture methodology developed for the US Army's Future Force could be adapted to the requirements of Civil Support, Homeland Security/ Homeland Defense. This architecture links the sensors, command and control, and communications systems of local, state, regional, national and DoD elements. The aim of the C4ISR is to, 'see first', 'understand first', 'act first' and 'ensure reliability'.

Command & Control: Decision makers will have access to a COP with timely updates to ensure near-perfect situational awareness. Information will be automatically provided as well as taken from the network. The system will use forward sensor fusion and omnipresent assured network communications to enable improved battle management, command and control, and situational awareness. Information will be fused at the cutting edge to avoid information overload. Automated event-tracking capability will alert concerned agencies to various contingencies. Decision makers will be provided state-of-the-art collaborative, distributed, real-time decision aids to facilitate informed decisions.

Computer Systems: Computer systems will be designed to enable individuals to be recognised by any system and to be uniquely identified with appropriate status, priority, and information needs. The system will be integrated, interoperable, and interfaced with all concerned agencies. The plans will be continuously updated with inputs from higher and lower echelons as events unfold. The command post will be wherever the decision makers are located. Automated synchronisation of all actions and reconnaissance, surveillance, and target acquisition (RSTA) will be provided. Computer hardware will be robust and rugged for operations in all types of environment. It will be modular for ease of repairs or for upgrades and will be protected against hostile penetration with advanced firewalls and other security systems. Software applications will be robust and flexible.

Communications: The network will use ground, airborne, and space communication line-of-sight and non-line-of-sight links to achieve continuous, uninterrupted connectivity on the move with minimum risk of being picked up by the hostile elements. Entities will be provided where required and connected to the network for exchange of information. The network should facilitate identification of friendly elements and access to national grid. Network management should be essentially built in, requiring little to no on-site support. The network should be self-configuring, allowing entities and nodes to enter and leave automatically without operator involvement. It will make maximum use of all available spectral bandwidth by dynamically adapting to the operational situation and allow voice, data, and video. Network protocols will facilitate multiple levels of security and should be highly reliable and secure. Its hardware and protocols will be commercially based to the maximum extent possible in order to facilitate technology insertions as they evolve.

Intelligence, Surveillance & Reconnaissance: Manned and unmanned ground, air, and space systems will extend the horizon beyond the line of sight to provide continuous and omnipresent surveillance of the environment through both passive and active RSTA. The sensors should be able to operate in all types of environment and weather conditions. They should be able to see through walls in urban environment. The ISR system should provide means to detect mines, booby traps, Improvised Explosive Devices, and remotely detonated munitions. The system should be able to detect, locate, and identify hostile elements and systems through semi-automated means. Information collection, analysis and dissemination will be distributed via the network to prevent single-point vulnerability. Sensor data collected from both manned and unattended sensor networks will be processed, networked and fused into an integrated COP for better situational awareness.

Threat analysis and threat priorities should be carried out automatically or with the aid of software tools. Near-real-time friend or foe should be available. System should be able to see through decoys, deception, and disinformation. Robotic systems will be employed for certain high-risk situations. Capability must exist to defeat hostile ISR. The ISR system should also be able to manage the overall application of integral sensor assets.

INDIAN PERSPECTIVE

India has been fighting terrorism for almost two decades but so far there has been no central organisation on the lines of homeland defence of the US. India has had a fractured response to terrorism depending upon the situation. Most of the time the Indian Army has been involved in Jammu and Kashmir, and the North East. At times, local police is involved in the hinterland and in special situations such as Akshardham and Mumbai, SPG has been called. Some form of manual C4ISR does exist with the defence forces and the central police organisations. Some form of electronic intelligence is also available through central organisations. After the Mumbai attack, coastal surveillance is being tightened but air surveillance on the peninsular India is sadly lacking. There is no central organisation to synergise all aspects of homeland security. India needs to study the various models of the Army, Navy, Air Force and the US model to adapt a suitable one to meet its requirements.

To 'see first, understand first, act first, and finish decisively' in support of homeland security operations, a seamless C4ISR system which is multi-functional, multi-mission and has a flexible architecture is required. Situational understanding, information management, communications, detection and avoidance of hazardous areas, area denial, intelligence collection and dissemination are the important ingredients of an effective C4ISR system. The system should also be fully networked to have timely response time. ■

PHOTOGRAPHS: SP GUIDE PUBNS

'Focus is on C4I2 SYSTEMS'

Lieutenant General P.C. Katoch
Director General, Information Systems

SP Guide Publications (SP's): How is the IA visualising transformation to NCW?
DGIS: The IA is in a phase of transition from conventional warfare to information-enabled warfare, that is, from platform centric to NCW. The full realisation of any such revolution is possible only with technological development, organisational adaptation and, most importantly, a national will. An effective and technologically sound information technology (IT) force, along with robust communication networks, have been created to facilitate real-time sharing of information and quick decision making so as to achieve information superiority. A road map has been formulated by which we can progress steadily towards being a potent IT force.

Next, we have identified development of C4I2 systems as a major thrust area for modernisation of the army. Development and fielding of automated operational information systems for various levels of operations from Army HQ to Battalion HQ and down to individual soldiers is in progress. Command Information Decision Support System, Artillery Combat Command Control System, Battlefield Surveillance System, Air Defence Control and Reporting System and Battlefield Management System are the major projects under development. Integrated together with requisite communications, these systems will provide near real time 'sensor-to-shooter' links to make the army a network centric force.

SPG: What is the progress in NCW currently within the army and among the three services?
DGIS: The hurdles in sharing of information among various agencies of the country are not only because of lack of media or infrastructure to share the information, but due to organisational and procedural hurdles. Warfighting is a continuously evolving affair and a net centric enabled force is the requirement of the day. We are making headway towards achieving network centric force keeping the primary focus of protecting our borders and sovereignty. At present, we have a number of projects working towards obtaining NCW capabilities, which are following a road map and are at different stages of development. Even the networking at Tri Service level has been worked out and is being implemented.

'Enhancing communication a priority'

Lieutenant General P. Mohapatra
Signals Officer-in-Chief

SP Guide Publications (SP's): How are you planning to meet the Network Centric Warfare (NCW) needs of the Indian Army (IA) with the anticipated delay in establishing the Tactical Communication System (TCS)?
SO-in-C: The vision of the Corps of Signals is to attain and maintain informatics ascendancy by developing infrastructure to cater for NCW in a digitised battlefield of tomorrow. The aim and objective of the Corps is to facilitate the IA's march towards net-centricity. TCS, being a large and technologically intensive project, will take some time to fructify. In the interim, adequate steps have been taken to ensure that our objectives are met, albeit in a manner to conform to development of other systems and applications.

SP's: Enumerate the mobile communication needs of the army. How are these being met?
SO-in-C: Mobility is of essence, especially in the Tactical Battle Area. An infantry foot soldier needs to communicate with his platoon/company commander and up the hierarchy; so does a tank or an Infantry combat vehicle, a commander on the move or any other mobile subscriber. The Corps of Signals were the pioneers in mobile communications in both the civil and the defence arena with a mobile communication subset in Army Radio Engineered Network. Today, we have assimilated the CDMA/GSM technology. Technologies, like WiMax, are still in nascent stages of development and will be absorbed to ensure high data rates as voice and data would both be important constituents of communication for future wars.

SP's: How are you planning to provide connectivity for Command Information and decision Support System?
SO-in-C: The domain of enhancing communication in the tactical battle area and the facilitation of synergy of elements in tactical battle field is a priority for the Corps. The Corps is fully equipped and capable of meeting the requirements of the various systems being fielded in the IA. The Corps has established a reliable, responsive, robust, secure and consolidated infrastructure which is capable of filling pre-TCS voids and meeting both present and future communication related requirements of the environment.

45
1964-2009
SP GUIDE PUBLICATIONS
WIDENING
HORIZONS...

Experience Counts

> www.spsmilitaryyearbook.com
> www.spsaviation.net
> www.spslandforces.net
> www.spsnavalforces.net
> www.spsairbuz.net
> www.spshomelandsecurity.com

SP GUIDE PUBLICATIONS
www.spguidepublications.com

GREAT PERFORMANCES.

SMALL “ITEMS”.

DESIGN AND PRODUCTION OF ELECTRONIC DEFENCE SYSTEMS.

elt
mind is the first defence