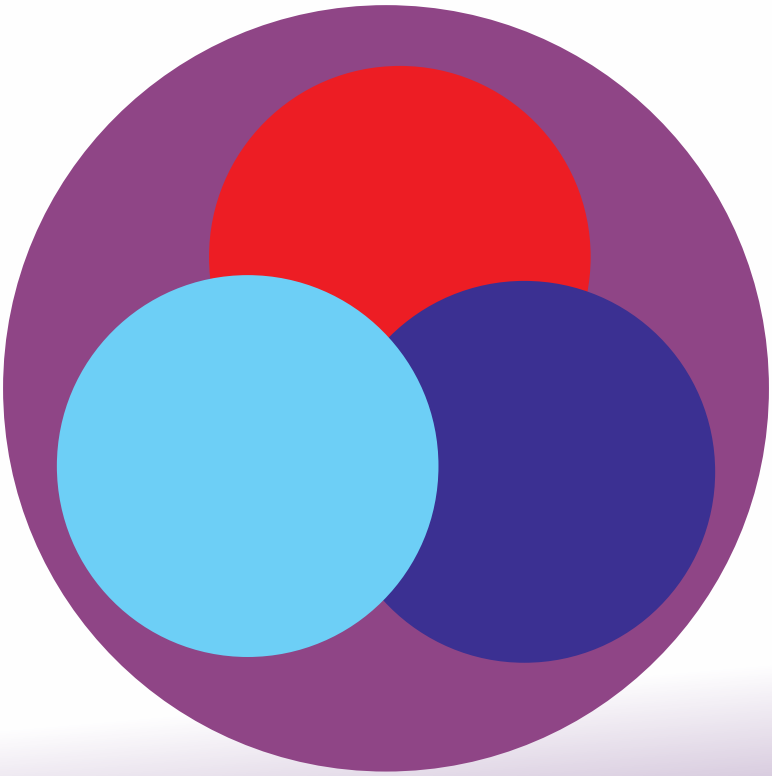
SYNERGY

Journal of the Centre for Joint Warfare Studies

Volume 1 Issue 1 ISSN : 2583-536X October 2022



JOINT MULTI-DOMAIN C4ISR FOR THE INDIAN ARMED FORCES

SYNERGY

JOURNAL OF THE CENTRE FOR JOINT WARFARE STUDIES

Volume 1 Issue 1 ISSN : 2583-536X October 2022

CENJOWS
(Established : 2007)
Room No 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road,
New Delhi - 110003 (INDIA)
Telephone Nos : 011-24364881, 24366485
Fax : 011-24366484
Website : www.cenjows.in
E-mail : cenjows@cenjows.in, cenjows@yahoo.com

ABOUT US

CENJOWS was raised in 2007 as an independent think tank, registered under the Societies Registration Act, 1860. This aims to promote Jointness as a synergistic enabler for the growth of Comprehensive National Power and provide alternatives in all dimensions of its applications through focused research and debate.

Year of Publication	:	Oct 2022
Frequency	:	Bi-Annual
Language	:	English
Publisher	:	Lt Gen Sunil Srivastava (Retd) Director CENJOWS 301, B-2 Wing, 3rd Floor Pt. Deendayal Antyodaya Bhawan CGO Complex, Lodhi Road New Delhi-110003
RNI Number	:	DELENG/2022/82424
Editor	:	Lt Gen Sunil Srivastava (Retd) (director@cenjows.in) 301, B-2 Wing, 3rd Floor Pt. Deendayal Antyodaya Bhawan CGO Complex, Lodhi Road New Delhi-110003

All correspondence may be addressed to:
Editor

Centre for Joint Warfare Studies (CENJOWS)
301, B-2 Wing, 3rd Floor, Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road, New Delhi-110003
Telephone: (91-11) 24366485/Telefax: (91-11) 24366484
e-mail: cenjows@cenjows.in / cenjows@yahoo.com
Website: http://cenjows.in

Price : Rs 300/- INR or US 15$

RNI No. : DELENG/2022/82424 Online ISSN : 2583-536X

JOINT MULTI-DOMAIN C4ISR FOR THE INDIAN ARMED FORCES

INDEX

JOINT MULTI-DOMAIN C4ISR FOR THE INDIAN ARMED FORCES

Foreword		-	**vii-viii**
From The Director's Desk		-	**ix-x**
1.	**Joint C4ISR for The Indian Armed Forces- Quo Vadis?** Lt Gen Sunil Srivastava, AVSM, VSM** (Retd)	-	**1-37**
2	**Redefining C4ISR & Adaptive Evolution of Digital Intelligence** Wg Cdr Srambikal Sudhakaran (Retd)	-	**38-42**
3.	**Geospatial and Data Fusion Technologies for Real Time Situation Awareness and Decision Making** Brigadier (Dr) Rajeev Bhutani (Retd)	-	**43-58**
4.	**Leveraging Technological Advances in C4ISR to Enhance Situational Awareness and Decision Making** Gp Capt Amitabh Mathur (Retd), Mr Sandeep Kumar Srivastava, Mr I Prabu	-	**59- 77**
5.	**Advancing C4ISR Capability: Leveraging Emerging Technologies And Commercial Advances** Gp Capt Puneet Bhalla	-	**78- 94**
6.	**Space Based Joint C5ISR Capability Building** Lt Gen A B Shivane, PVSM, AVSM, VSM (Retd)	-	**95-110**

7. C4ISR Architecture for An Integrated Air Defence and BMD- Necessity and Feasibility - 111-124
Air Marshal Daljit Singh, PVSM, AVSM, VM (Retd)

8. C^4I^2 SR In AD Theatre Setup - 125-133
Gp Capt RK Dhir (Retd)

9. Joint C4ISR and Future Ready Force - 134-152
(Brig (Dr) Navjot Singh Bedi, Brig PMO DCN & Cdr DCA)

10. C4ISR Set-Up in Maritime Domain Existing Systems, Challenges, Pathways for Futuristic Warfare Preparedness - 153-170
Captain (IN) Kamlesh K Agnihotri (Retd)

11. Utilization of Synthetic Environment For Defence Experimentation In Planning, Evaluation And Acquisition of C4ISR Systems - 171-183
Mr Manoj Tyagi et al.

12. Standardisation and Codification A Perspective for Defence Forces and Industry - 184-193
Cmde Gopal R Wani, Director, Directorate of Standardisation- MoD/DDP

Notes:-

- Views expressed in articles are individual opinions of the writers, and not of CENJOWS.
- Contributors to Synergy Journal are requested to visit the website for the theme of the next issue and guidelines.

Air Marshal BR Krishna
PVSM, AVSM, SC, ADC
Chief of Integrated Defence Staff to the
Chairman, Chiefs of Staff Committee
& Chairman CENJOWS

FOREWORD

Command, control, communication, computers, intelligence, surveillance, reconnaissance (C4ISR) is a system of systems that helps enhance situational awareness and decision-making ability of commanders, while also facilitating better operational planning and execution. Rapid advancements in digitally empowered information and communication technologies have enabled commensurate advances in C4ISR components and networking capabilities.

At the same time, the transformation of the modern conflict zone from a linear battlefield into an expansive battlespace, spanning multiple domains and dimensions, has placed greater demands on the cognitive aspect of warfare. Recent campaigns have highlighted the edge that technologically superior C4ISR provides at all levels of conflict and there is now a greater acceptability of the impact of C4ISR capabilities on military doctrines. The decision makers are seeking more optimised sensor geometries to enhance coverage, as also real time flow of information through secure, pervasive communication networks, to achieve information superiority. Advanced digital tools and data processing capacities are being harnessed, which would help streamline decision making processes and shorten the OODA cycle.

All modern military operations involve collaborative action, and synergistic application of combat power dictates networked C4ISR components. However, these capabilities have been traditionally developed in isolation to cater to specific domains or functions. These service-centric, closed architectures preclude interoperability and joint operations. While all legacy systems would need to be integrated through appropriate protocols, the

future development paradigm for such systems would explore opportunities provided by emerging technologies towards enabling integrated or interoperable architectures and enhancing the systems' prowess.

The U.S. has been the earliest practitioner of this concept and has maintained an edge through consistent investments and innovation. It is pursuing joint all-domain command and control (JADC2) in earnest, to include emergent technologies and their applications, with an aim to achieve and maintain information and decision-making superiority. In China, information dominance has been a defining factor of its military doctrine, which has now evolved into "intelligentisation", with special emphasis on exploring artificial intelligence (AI) and quantum computing to augment C4ISR capabilities. Both Russian and Ukrainian C4ISR are being studied, evaluated and discussed for their efficacy. Globally, investments into capability enhancements of C4ISR systems are seeing an upward trend.

Indigenous efforts in terms of sensor diversification and scaling, improving interoperability among systems and achieving network centricity have also intensified in recent years. The intrinsic strength in Information Technologies is being exploited to provide futuristic, innovative solutions. 75 AI based products and technologies designed and built through government and private industry involvement, of which 15 were related to C4ISR, were recently launched in July 2022. The Atmanirbharta efforts would not only incentivise domestic industry, but also ensure robustness and resilience of systems. Most importantly, systems would get timely upgrades without any contractual complexities.

This issue of Synergy, in its continued quest to address issues related to National Security and joint operations, has comprehensively covered various aspects related to the technology intensive military C4ISR systems. I am sure the readers will benefit by getting an in-depth look into this complex domain and would be instrumental in providing more clarity for the path ahead.

(BR Krishna)
Air Marshal
CISC & Chairman CENJOWS

Lt Gen Sunil Srivastava, AVSM, VSM (Retd)**
Director CENJOWS

FROM THE DIRECTOR'S DESK

Putting together this issue of 'Synergy' on the theme "Joint Multi-domain C4ISR for the Indian Armed Forces" has been an exciting experience. The theme was shared with our audience and evinced a very encouraging response, which does not surprise us, since lessons of the ongoing and recent conflicts have yet again underscored the *salience of multi-domain shared situational awareness and collaborative, machine assisted decision making,* at all levels of warfighting. C2 (Command & Control and C3&4 (Communications & Cyber), dictate and define the span and speed of ISTAR capabilities- *finding, fixing and finishing. The operational environment demands a flatter and flexible multi-domain architecture, supported by resilient and redundant communication technologies and topologies, to enable "intent driven joint war-fighting"*, at an operational tempo that outmatches that of the adversary.

We have taken a wide sweep and put together well researched articles, authored by *domain experts, professionals, scientists and academics.* The readers will be enriched by reflections on C4ISR concepts and capabilities of leading and Indian Armed Forces, the *requirements and challenges inherent in developing Joint C4ISR capabilities for the proposed Theatre Commands and pathways for expeditiously addressing the impediments* of interoperability, security, cultural and procedural stovepipes. New perspectives on *redefining C4ISR and*

digital intelligence, C4ISR concepts for integrated AD/ BMD and AD Theatre Setup, and nuances of C4ISR for Space and Maritime domains will be of great interest to the readers. Professionals have suggested pathways for *leveraging technologies and geospatial capabilities to enhance C4ISR capabilities* for a Future Ready Force. A unique feature is an insight into *utilization of synthetic environment for planning and evaluating C4ISR Systems*.

We hope to ignite an informed debate to spur Joint Multi-Domain C4ISR initiatives, so as to achieve the decision superiority needed for victorious outcomes.

Happy Reading!

(Sunil Srivastava)
Lt Gen (Retd)
Director

JOINT C4ISR FOR THE INDIAN ARMED FORCES- QUO VADIS?

Lt Gen Sunil Srivastava, AVSM, VSM** (Retd)*

Abstract

The Indian Armed Forces drew the first blueprints for Service specific C4ISR solutions almost four decades back. While Service specific C4ISR systems have been fielded, the only joint projects to have been fielded so far are Defence wide communication networks. This article critically analyses the salience of Joint C4ISR in the modern warfighting, the challenges and lessons that must be learnt from own and global C4ISR concepts and architectures, the C4ISR requirements for the proposed Joint/Theatre Commands, and the pathways that must be adopted post haste.

The Operational Context and Environment

The operational environment demands speed and agility, since time is at a premium for leaders to analyse a sea of information and act decisively. Thus, the need for speedy acquisition, dissemination and processing of information, and collaborative decisions lies at the heart of C4ISR systems. We are faced with two collusive adversaries, each capable of prosecuting fast paced operations with ever increasing precision and reach, spanning all domains. The PLA doctrine of ‘systems warfare’, places a premium on targeting of systems and decision nodes, which

exploits the increasing vulnerabilities in space, electromagnetic spectrum (EMS) and cyberspace. Both sides are leveraging capabilities in air, EW and space domains to destroy traditional platforms like aircraft, tanks and guns, in the ongoing operations in Ukraine, especially where there is a lack of multi-domain synergy.

The Joint C2 Paradigm and C4ISR

Before analysing the challenges in Joint C4ISR, a brief examination of C2 would be appropriate, since this is the point of departure for varied acronyms like C6I2SR. Simply stated, C2 is the authority of a commander to command and task the allotted resources. In a joint context, it entails optimal application of resources to achieve joint combat missions, during competition, crises or conflict. C2 systems leverage technologies and topologies to cyclically perform observe, orient, decide and act (OODA) functions. C4ISR (Command, Control, Communications, Computers, Intelligence, surveillance and reconnaissance) together support the OODA functions, providing essentially two outcomes- Shared Situational Awareness (SSA) and collaborative decision-making (DM). Expanded terms like C6I2SR reflect additional functions like Cyber-security, Combat-systems and Interoperability. An Air Defence system is typically a C6I2SR system. C4ISTAR includes targeting as well and makes the sensor-DM-shooter chain complete. In this article, C4ISR implies C6I2STAR contextually.

Joint C2 Evolution-From Network Centric Warfighting (NCW) to Multi-Domain Operations (MDO). Operations of two Services primarily coordinated at the theatre/operational level is a narrow perspective of Joint operations. Advances in ICT technologies have helped C2 concepts evolve from NCW, which leverages connectivity between sensors-DM-shooters, primarily within a Service/domain, towards MDO which envision a joint C4ISR architecture which spans across multiple domains, ensuring an optimal exploitation of capabilities. Essentially,

C4ISR envisages an effective Battle Management Systems (BMS) having dynamic cross-domain integration of sensors/effectors in the physical domains, data integration/analysis in the information domain, and making sense and decisions in the cognitive domain. Cyber, EMS and psychological effects, together make up the information environment (IE). Information and communications are key to decision superiority. Theatre C4ISR needs to be joint at all levels, so as to graduate from plan driven operations to intent-driven operations, enabled by command of multi-domain capabilities. IR 4.0 technologies (AI, ML, big data, cloud, 5G, quantum) have bolstered multi-domain integration and C4ISR functions like bulk information processing, storage, distribution and machine assisted DM. A Joint C4ISR system presupposes joint C2 structures, doctrines, interoperable sensors/systems, interoperable, secure and redundant networks, and secure AI/ML driven data centres, breaking the enduring cultural barriers to interoperability. Joint Staff typically includes experts from all domains to perform Joint functions (C2, operations, intelligence, fires and sustenance). The essence is to compensate for domain vulnerabilities, while targeting those of the adversary, and disrupting his OODA cycle, compelling him to choose undesirable options. Instead of a capability overmatch, victorious outcomes should be achieved through synergetic and convergent operations of dispersed, manned and unmanned entities in multiple domains, leveraging interoperable C4ISR systems-of-systems (SoS).

C4ISR and MDO Concepts- Leading Militaries

Russia. Russia is actively leveraging capabilities in the information, cyber, electronic and space domains to enable the physical domains. Russia's multi-domain and reflexive control strategies are centered on information warfare (IW) to shape and control the adversary's behaviour and the strategic environment. While the West considers non-military measures to be ways of avoiding war, Russia considers them part of war[1],

and form part of its non-linear strategy in the competition phase[2]. Russia's theory of war posits the adversary is a system with key sub-systems[3]. It also has reinforcing concepts like New-type Warfare, reflexive control and reconnaissance-fires complex to shape the adversary's behaviour[4]. In 2019, Russia claimed a breakthrough in its C4ISR systems, which leverages AI and Big Data technologies to provide SSA with decision options, as part of an automated control system (ASU)[5], at all levels, from tactical to strategic. Its Akatsia-M sub-system interacts with systems of the Maritime Fleet, Aerospace Forces and the Airborne Forces, and exchanges real time information with the National Center for Defence Management in Moscow[6]. Russia is also increasing the automation in AD systems, C2 and testing of strategies, to make data collection and decision-making more efficient[7]. However, effectiveness of the Russian systems is reported to have been suboptimal in the ongoing Ukraine operations.

China (PLA). The PLA envisages warfighting as a multi-domain confrontation between competing SoS. PLA seeks to dominate the competition phase with theories of Unrestricted Warfare and Three Warfares. Unrestricted warfare challenges concepts which aver that warfighting is a quick contest, leveraging technology. PLA's concept of high-intensity warfighting has evolved overtime, and is centered on concepts of informatised and intelligentised warfares and multi-domain systems confrontation (target-centric warfare), by enhancing its capacity and capability for confrontation, especially in cyber, space, EMS and the cognitive domains. The PLA is enhancing integration between all levels of command, as part of its integrated joint operations (IJO). Systems confrontation prioritises targeting of the linkages and nodes of a NCW capable force, over destruction of individual military platforms.[8] PLA, like Russia, places emphasis on destruction of C4ISR systems, labelled A2AD (Anti-Access Area Denial) strategy by the West, to gain decisive information advantage in the early stages of conflict. The evolution of

Chinese Command Automation Systems (C4ISR) has been guided by integration, centralisation, peacetime/wartime use and innovation. PLA is developing information offence and defence, situational awareness, command decision making and precision strikes capabilities at a fast pace. PLA has been using multi-layered digital communication systems, from strategic to company levels, since more than a decade. PLA had likely fielded a Joint Operational Data Link (ODL) system called Tri-Service Tactical Information Distribution NW (abbreviated as TIS, similar to the JTDIS of the US), delivering secure data and voice, across different communication technologies. TIS possibly has nodes linked via satellites, OFC, Services/Tactical NW and relay aircraft, allowing the Campaign Command HQ and tactical units to share theatre-wide battlefield picture[9]. PLA aims to attack critical networks through kinetic and non-kinetic means, leveraging multi-domain structures like the Strategic Support Force (SSF), that integrate space, cyber and EW, psychological warfare missions. Harnessed Lightning[10], a 2021 report, has listed seven application areas of AI, mostly C4ISR related, in descending order, based on the value of contracts- Autonomous Aerial and Sub-surface vehicles, ISR, Predictive maintenance and logistics, IW and EW, Simulated training, C2 and automated target recognition. PLA intelligentisation is infusing autonomy in C2 through unmanned platforms/swarms and drone mother ships.

The US-Joint All-Domain Command and Control (JADC2). The Air Land Battle concept led to dual domain integration of capabilities, with concurrent jointness in doctrines, strategies, structure, equipment, and training. The subsequent concept of Air Sea Battle (ASB) was followed by MDO, a natural progression from joint warfighting. MDO challenges the A2AD systems which threaten the freedom of manoeuvre in all domains. The US military has the most advanced C4ISR systems, but the extant tactical C4ISR systems of the three Services have interoperability constraints. JADC2 is a component of the Joint Warfighting Concept.

JADC2 performs three C2 functions- sense, make sense and act, which make MDO possible. It would enable the Joint Force to leverage automation, AI, predictive analytics and ML to deliver informed solutions via a resilient network environment11. An implementation plan has been put in place in March 2022, to execute the JADC2 Strategy (June 2021)). JADC2 accelerates the decision cycle, improves the resilience of C2 systems, better integrates conventional and nuclear C2 procedures and enhances interoperability12. To implement JADC2, the Air Force is developing the Advanced Battle Management System (ABMS), the Army is developing Project Convergence and the Navy, Project Overmatch13. Tri-Service field experiments are being held since 2019. The US Army's Warfighter Information Network-Tactical (WIN-T) is perhaps been one of the largest C4I program in the world[14]. However, not all Joint C4ISR endeavours have succeeded, eg the Army's Joint Tactical Radio System (JTRS) foreclosed in 2011[15]. Another program that went awry was the Joint Enterprise Defence Infrastructure (JEDI), which has been retendered as Joint Warfighting Cloud Capability (JWCC)[16].

Joint C2 Models- The Indian Experience

Strategic Forces Command (SFC). The unique C2 model of the SFC is tailored for strategic nuclear deterrence. It is a Tri-Service, geographically dispersed and multi-layered organisation. It has a nuanced Strategic C2, which renders it unsuitable for replication in the conventional field forces.

Andaman and Nicobar Command (ANC). Formed in 2002, the ANC is a microcosm of the envisioned future joint theatre commands. Though ossified Service cultures have stymied the efforts to infuse true jointness with integration of joint C4ISR, some progress has been made in the recent past. The operational control of the Indian Coast Guard (ICG), three Component Commanders under a Joint Chief of Staff, heterogeneous staff billets, fielding of Tri-Service Software Defined Radio (SDR), exploitation of Defence Communication Network (DCN) and a

functional Joint Operational Centre (JOC), are notable achievements. Quite evidently, C4ISR frameworks are cemented as much by trust**,** as through technological interoperability. Experiences of ANC provide guidance and lessons for the Joint Theatre Commands (JTCs) on the anvil. ANC is an ideal test bed for all Joint C4ISR initiatives.

Status of Development of C4ISR Systems- Indian Armed Forces

The Indian Air Force (IAF). It developed and fielded Tactical AD Information Display System (TADIDS) in the late 1990s. With operationalisation of AFNET digital NW in 2010, Integrated Air Command Control System (IACCS) replaced TADIDS. It integrates airborne and ground based sensors, weapons and C2 nodes of IAF, besides civil and coastal radars, to generate an integrated Recognised Air Situation Picture (RASP) and generate engagement geometries. The IAF upgraded the AFNET and also deployed 3G/4G based AFCEL cellular network in 2013. GSAT-7A, launched in 2018 (30% payload shared with the Army), enhanced the communication bandwidth capabilities. GSAT 7C, to be launched in 2 to 3 years, will bolster the NCW capabilities, with secure BLOS and SDR capabilities. The IAF has acquired the critical Operational Data Link capability with SDR, to enable secure high speed voice/data/video communications between ground and aerial platforms and C2/IACCS nodes[17]. This was corroborated by a former Chief of Air Staff[18].

Indian Navy (IN). MDA information of aerial and surface objects comes from shore, ship or space based sensors of various types. The IN fielded 'SANGHARSH', a sensor-grid MDA application developed in-house in 1996, which later evolved into Trigun, a pan-Navy C4ISR military-MDA solution, developed by DRDO. The first phase was completed in 2012, the second in 2021 and completion of third phase is envisaged by 2024[19]. The IN has also fielded a National Command, Control, Communications and Intelligence (NC3I)[20]. Besides, a National

Automatic Identification (NAIS) by the Directorate General of Lighthouses and Lightships (DGLL), a Vessel and Air Traffic Management System (VATMS) by ONGC, a Long Range Tracking and Identification (LRIT) System by DG Shipping were developed, largely for non-military MDA[21]. The Information Management and Analysis Centre (IMAC), a nodal centre for NC3I, was set up in 2014 and Information Fusion Centre-Indian Ocean Region (IFC-IOR) in 2018. DG Shipping proposes to set up a Mercantile Maritime Domain Awareness Centre (MM-DAC) and is developing indigenous software for Vessel Service Traffic (VTS), which would augment NC3I. The IN is leveraging AI/ML and big data analytics in Trigun System with full integration planned by 2024[22]. The Naval C4ISR systems ride on the enterprise wide NEWN network, which is has been upgraded to Navy Communication Network (NCN). SDRs to meet its varied requirements, have been developed and are being deployed by the IN[23]. Communications of the IN were augmented by GSAT 7, launched in 2013, which will be replaced by GSAT 7R in 2023. India also has a Coastal Surveillance Radar System (CSRS) with radars across Seychelles, Mauritius and Sri Lanka, with plans to extend it to other countries in the region[24].

The Indian Army. It embarked on expansive and ambitious C4ISR projects almost 4 decades back. However, their realisation has been relatively less promising. While it has a robust pan-India ASCON static, secure, state-of-the-art, multimodal, high bandwidth NW connectivity, the plan for a mobile and secure Tactical Communication System (TCS) has been in doldrums for over 2 decades[25]. It also fielded a Mobile Cellular Communication Network (MCCS), based on 2G, in parts of J&K in 2007, and a 3G based MCCS in the Kashmir Valley in 2016. A Mobile Integrated Network Terminal (MINT), a 4G LTE based Network solution, is under development[26]. The initial conceptualisation of Tac C3I systems, cast almost four decades back, was holistic and ambitious. Certain projects like ASTROIDS (Corps and above), CIDSS (Brigade

to Corps) were partially implemented, ACCCS (Artillery Fires System) has been deployed, BSS (Battlefield Surveillance System) is at an advanced stage of trial evaluation, EW and ELINT have been fielded. All these are standalone systems. ADC&RS (Akashteer- Air Defence Control & Reporting System), which will have an interface with IACCS, has recently been approved as a project for BEL in Dec 2020. At the Soldier and battalion level, Project F-INSAS (Future Soldier as a System) was conceived in 2005, with plans to network the soldier. The NW requirement was later merged with BMS (Battalion level C4ISR), which was progressing concurrently since 2002. However, consequent to foreclosure of BMS in 2017[27], a project for SDR communications for F-INSAS is at an advanced stage. The future vision is to seamlessly integrate operational and management applications through army-wide Indian Army Information System (IAIS), catering for peace and war time functions. An in-house capability to leverage APIs for integrated solutions has been developed and Message Oriented Middleware (MOM) are being evaluated to enable interoperability of legacy systems and future systems[28]. INDIGIS, an indigenous GIS has been developed by DRDO[29], which will bolster interoperability. Information is shared pan-Army through secure file-sharing and messages over the Army Data Network (ADN), integrated with software solutions and a Common Operational Picture (COP) is updated on digitised maps. A secure Cloud and digi-locker service, for computing and storage, was launched for the Army in July 2018. It will enable information being accessed by authorised users, pulled when needed, and pushed where mission critical. GSAT 7B, to augment the communication needs of the Army, has been approved to be launched in 2-3 years.

Tri-Service C4ISR Capabilities.

ISR Capabilities. They leverage satellites, UAVs, AWACS, AEW&C, aerostats, maritime surveillance, EW and ELINT (SIGINT & COMINT)

assets, are quite robust. However, joint accessibility, sharing, integration and imagery analysis for enabling a multi-domain, Service agnostic SSA and collaborative decision-making, is long overdue. A VOIP based, Audio and Data Management System (ADMS) has been developed for surveillance platforms. It interconnects regardless of radio band, frequency and hardware and can be used by all Services[30]. To provide near real time intelligence, and dynamic time-critical targeting of moving ground and maritime targets, an airborne Intelligence, Surveillance, Targeting & Reconnaissance System (ISTARS), with SAR, GMTI, ELINT, COMINT, EO/IR and communication capability, is being developed by DRDO. It will be a SoS, with airborne and ground segments[31]. The platform can provide ISR over land borders, maritime and littoral areas. It also performs BMS and C2 tasks, fusing inputs from multi-spectral sensors[32]. A National Geospatial Intelligence System, integrating all stakeholders, is under implementation at an accelerated pace.

Joint Communications

DCN. The first integrated, highly secure, scalable communication NW, DCN, was launched in June 2016, enabling the three Services and SFC to share SSA for faster DM. It has a pan-India reach, including island territories.

NFS. NFS, a Tri-Service NW, in exchange for 2G/3G spectrum vacated by the defence forces, is nearing completion. It has a OFC backbone, with microwave, radio-relay and satellite components and NW management systems.

Joint SDR. A tactical Joint SDR is at a trial and development stage.

Extant propriety and legacy C4ISR systems are service-centric, mission-specific and not-interoperable. These standalone systems process large volumes of information, both own and enemy, but do not present a curated tri-Service picture. Even within a Service, systems with propriety HW/

SW lack interoperability, precluding backward and forward integration. A joint, real-time, SSA remains an elusive ambition. Often, warfighters share operational information on voice systems, which is interference prone, insecure and inefficient. The challenges are further compounded by lack of NW interoperability between AFNET, NCN and ASCON. This challenge is likely to be addressed shortly.

Case Study- Integrated AD (Tri-Service)

An Integrated AD System (IADS) has 3 basic components, viz, surveillance, BMS and weapons control. Joint C4ISR for IADS would entail integration of these varied sub-systems from different services across multi-layered communication architectures. Joint C2 of IADS would entail seamless integration between BMS nodes of IACCS, Trigun and Akashteer. The Joint Indian Armed Forces Doctrine (2017)[33] only mentions the Air Force elements embedded at the Army and Naval Command HQs, in form of Advance HQ, and Maritime Air Operations Centre, as well as Tactical Air Centers (TAC)/Ground Liaison Sections (GL Sections) and Maritime Element of Air Force, at the tactical levels. The doctrinal issues and organising principles related to Integrated AD and Air Space Management have been comprehensively outlined in the Joint Doctrine for Air-Land Operations[34]. This document comprehensively outlines principles, procedures and responsibilities for a harmonised and coordinated AD framework between the three Services. The Union War Book was revised in the mid-1990s, and stipulates that, the responsibility of providing AD of Indian Air Space rests with the Indian Air Force, encompassing India's landmass, island territories, territorial waters and the air space above them[35]. The responsibility of AD is shared by 5 geographical Commands of IAF, through ADDCs, and controlled by the automated IACCS. It has been argued that inadequacy of multi-role aircraft rules out creation of a centralised AD Command (ADC) till the IAF does not reach the desired strength of 42 squadrons, also citing

the limited availability of AWACS, AEW&C and Flight Refuelling Aircraft (FRA) as a reason[36]. The CDS was mandated to create theatre/joint Commands by end 2022. The mandate of the ADC, its structure and contours, and de-confliction of its role with the Ground-based (Land Forces) AD in the Tactical Battle Area (TBA), the mandate of future JTCs, and various doctrinal, functional, procedural and asset sharing challenges, are being resolved by a high level tri-Service committee. Meanwhile, defence analysts and senior leaders have voiced mixed reactions about the desirability of ADC[37] [38] [39] [40]. Presently, the IACCS is yet to be integrated with Trigun and Akashteer (upcoming) systems**.**

The US Concept- NORAD[41]. The NORAD (North American Aerospace Defence Command), is mandated for defence of the aerospace of Canada and US. In 2006, the Maritime dimension was also added. The Command centre of NORAD is co-located with US Northern Command (created in 2002, AOR also includes Mexico), and both have the same Commander. It has Regional Centres for Alaska, Canada and Continental US. Air Force North (1st Air Force), part of the Air Combat Command (ACC), is the Air Component Command of the USNORTHCOM. 1st Air Force is the Senior Agency in the Theatre Air Control System (**TACS**)[42]. It has 9 or 10 aligned Air National Guard Fighter Wings, which handle almost 90% of the AD missions. Some Active Duty Force members and Air Force Reserve also form part of the 1st Air Force. The takeaways are that the US has a Bi-National AD Command, which has three Regional sub-divisions. It is also truly tri-Service, since it encompasses MDA as well. While the Air Force is the Senior Agency in the TCAS and the assets primarily belong to Air National Guard. Defensive Counter Air (DCA) and Offensive Counter Air (OCA) both are under one agency, the TACS.

The Soviet IADS Model. The Soviet AD Force was merged under the Air Force in 1998. Subsequently, in 2011, the Air Armies were renamed Air and Air Defence Armies (AADA), one each for the four Joint Strategic Commands (JSC)/Military Districts (MD) and the Northern Fleet. In 2015,

the Air Force was combined with the Space Force, creating an Aerospace Force (VKS). The AADAs have 3 types of Combat Arms- Air Forces, Space Troops and Air & Missile Def Troops (radars, S-300/S-400)[43]. Beyond the jurisdiction of AADAs, the VKS has 1st Spetsnaz Army, which commands AD Divisions (S-300/S-400) and a BMD Division, placed around Moscow and 15th Spetsnaz Army, based at Moscow, which oversees cosmodromes and space control/Surveillance/Missile-warning Centres[44], and is also responsible for GPS and space based ISR. In addition, Ground Forces of JSC, have AD assets integral to Combined Arms Armies/Tank Armies (SAM Brigades) and Army Corps (SAM Regiments). Key takeaways are that Russia has AADA directly under the C2 of JSCs, and DCA and OCA, both are under the Joint Strategic Commands. The Land forces AD resources have been well integrated in the Joint AD C4ISR. In the ongoing Ukraine conflict, and it is evident that VKS has had limited success in suppressing the relatively weaker Ukrainian Air Force. It has been speculated that the Russian strategy places strategic AF and OCA tasks lower than land operations and DCA. Adequate facts are not known as yet to conclude if the perceived failure of the VKS was due to shortcomings of the Joint C2 structures or due to pilot training and the state of equipment. Some analysts have also been skeptical about collaborative engagement capability of the VKS in joint engagement zones, across different Services[45].

China- The PLAAF AD Concept. The PLAAF Integrated AD System (IADS) took shape after the modernisation drive of the 1990s. PLAAF has 4 prioritised missions/tasks- Taiwan Invasion, Air Defence, Counter Intervention and Nuclear Deterrence[46]. PLAAF was organised into 5 Theatre Command Air Forces (TCAF) with radar, SAM and fighter aviation brigades, placed under six AD Bases in 2017[47]. AD Bases are directly subordinate to TCAF and each AD Base is responsible for the C2 of aviation Brigades, SAM and Radar units in their AOR, and coordinates joint training with PLAA/PLAN units. Some limited assets like transport,

bombers and special mission aviation units have been retained directly under PLAAF HQ. While AD Bases are primarily responsible for AD in their AOR, major offensive strikes and Joint Fires capabilities are with TCAFs. The three Theatre Command Navies (TCN), placed under the respective coastal Theatre Commands (Northern, Eastern and Southern), are responsible for AD of 3 regions surrounding Qingdao, Ningbo and Zhenjiang, and have radar and SAM brigades placed under command. The mission of the PLA Army AD units, equipped with MANPADS, AD guns and SAMs, is to provide point defence of land forces, but these may also support the overall theatre AD. PLA Army AD units have digitised the AD C4ISR and have Joint Data-links with Base/TCAD AD architecture. The integral AD Brigade of the Group Armies may be under its direct operational control or it may be placed under the Theatre Air Component Commander for short periods. However, realtime joint engagement capabilities remain a challenge, especially in maritime joint engagement zones[48]. Key takeaways are that post 2016, PLAAF HQ does not form part of the AD chain of command[49]. AD is the responsibility of 5 TCAFs, directly corresponding to 5 PLA Theatre Commands. AD of the Nation is a shared responsibility with PLAN in coastal regions. It also appears that routine DCA has likely been decentralised to AD Bases while OCA is under TCAFs. PLAAF clearly prioritises a geographical task-Taiwan and AD. However, writing about PLA C4ISR systems in 2020, PLA experts[50] have lamented a low degree of integration and coordination between various Services.

Deductions. The US, Russia and China have made their Air Forces responsible for AD of the air-space, further divided into regions/theatres/commands, much like Regional Air Commands of IAF. However, the Russian and Chinese have the regional AD C2 AOR identical with the Joint regional AOR, and are placed directly under the Joint C4ISR architecture at the theatre level. In the Indian context, geographical jurisdictions of Army and IAF Commands are at variance. In the Maritime sphere, the

Chinese and Russians Fleets have the AD responsibility of their AORs during peace/war, and NORAD takes it to the next level, where maritime areas are subsumed with NORAD. In India, IN is only responsible for Naval assets at sea during peace or war. The C2 arrangements of ICG will need a review post creation of Maritime. Our approach contrasts with the models adopted by Russia and China, which have made Navies/ Fleets responsible for coastal areas, both in peace and war, obviating any transition- a decision difficult to make in grey situations. Another fact that emerges clearly is that technology available today facilitates interoperability of critical C4ISR assets even between Nations (US and Canada), without impinging on sovereignty. The main enabler is trust and confidence in the system, technology, processes and institutions.

It is also evident that while vast geographies defy centralised AD C4ISR, technologies facilitate centralisation. Doctrinal concepts like layered AD, relative priority of strategic roles, flexibility and reach of multi-role aircraft and limited aerial resources for DCA/OCA advocate adoption of a centralised C4ISR approach. However, such arrangements presuppose ideal connectivity, with little or no latency. Fluid operations in degraded communication environments and lack of digital links between IACCS and mobile land-forces AD, advocate a decentralised architecture in the TBA. Joint digital communications with adequate BW are especially critical for the mobile AD systems in the TBA, with the BMS nodes of land forces AD elements in the TBA exercising minute to minute control, augmented by time, height and routing driven de-strategies, duly coordinated with IACCS based ADDC. Secure datalinks between ground forces and aircraft will preclude fratricide. Such models could be ideal precursors for the evolving C4ISR of the BMD, a more critical system.

Challenges Inherent in Developing and Deploying Joint C4ISR Systems

Development and fielding of Joint C4ISR systems universally faces three

major **challenges- interoperability, security and legacy service-centric cultures**. These challenges need to be addressed throughout the life of C4ISR systems.

Interoperability. Essentially, it is the ability to provide, accept and use services, to operate effectively together. Interoperability can be achieved through joint doctrines, concepts, data standardisation and compatible communications. Operational interoperability[51] goes beyond systems to include people and procedures. Technological Interoperability[52] is a pre-requisite for operational interoperability. It encompasses applications for interconnection, exchange and interpretation of data.

Interoperability vs Other System Requirements. Competing attributes dictate a judicious trade-off between the need for interoperability and other requirements like the need for security. Interoperability is also invariably accorded lower priority in face of constrained budgets.

Interoperability With Other Nations. The COMCASA (Communications Compatibility and Security Agreement), was signed with the US in 2018, though an earlier variant, called GSOMIA (General Security of Military Information Agreement) had been inked in 2002. COMCASA enables procurement and use of communication equipment for various platforms of US origin. The BECA (Basic Exchange and Cooperation Agreement), inked with the US in 2020, enables exchange of realtime geo-spatial intelligence and supply of high-end equipment, including sharing of geomagnetic data, nautical and aero-nautical charts, maps and other imagery. This helps enhance the accuracy weapons/platforms.

Why Interoperability In C4ISR Systems Is Challenging

Large militaries universally face systemic challenges outlined below-

- Inherent dilemma between current and future needs and between single and Tri-Service priorities.

- Systems / weapons / sensors invariably have new interoperability needs which cannot be anticipated, eg need to integrate new missile with different geospatial protocols on an AD system.
- New Joint C2 Structures necessitate new C4ISR interoperability needs, eg ANC and proposed JTCs.
- Propriety and legacy systems demanding integration.
- Technological obsolescence in the ICT field.
- COTS Technologies with open architectures are interoperable, but have security inadequacies.
- System upgrades in systems of one Service could impact joint interoperability.
- Varying pace of development of interdependent C4ISR systems and frequent design changes in C4ISR architecture results in interoperability mismatches. Fielding even similar aircrafts/helicopters over 15-20 years entails upgrades for C4ISR of the initial versions.
- Lack of organisational and doctrinal interoperability.

The Security Challenge

While open architectures and enterprise solutions are desirable, these come with questionable military grade security. A worry is backdoors in embedded chips and micro-electronics, which can only be overcome with a zero-trust strategy. This, in turn, presupposes an indigenous semiconductors chips manufacturing capability, for which the Government has taken a recent policy initiative[53]. The Defence Cyber Agency (DCyA) could be incorporated in the design and development process of C4ISR systems from a security perspective. SecDevOps must

be the preferred development approach. For addressing communication interfaces, DRDO must define standards for each of the 7 OSI layers, which the Indian OEMs/Partners could be licensed to use. DCyA must also conduct vulnerability analysis for Joint C4ISR systems.

Legacy Service-Centric Cultures

This is the biggest stonewall, as is evident from the aborted or botched C4ISR cases the world over, as also from our own experience in single Service cases like the Army's BMS and TCS. It stems from the stovepiped visions of fighting in and maintaining autonomous control of respective Service domains. They refuse to concede that every Service today has ever-growing ownership of multi-domain platforms, and together with the ever increasing interdependence on space, EMS and cyber domains, no single service can control or influence outcomes in its own domain by itself. Moreover, the traditional fixation and attraction towards big fighting platforms like ships, tanks and aircraft, relegates C4ISR capabilities to a lower priority, since given the constrained budgets, no Service wishes to prioritise tri-Service C4ISR capabilities. The Services also do not wish to see their projects delayed or derailed for want of interoperability. Tri-Service ownership of data standardisation and digitisation policies needs to be prioritised. Even the tri-Service secure DCN, is likely under-exploited. We need a culture that recognises the salience of Joint C4ISR systems. Yet another cultural challenge is the lack of understanding of procurement of digital and ICT assets, and requirements are constantly revised, given the desire to seek better returns on investments.

Joint C4ISR Capabilities Needed for Joint Theatre Commands (JTC)

We are at the cusp of taking a leap of faith to conceptualise and operationalise JTCs. It will be pragmatic to identify and evolve joint C4ISR systems and functions, for which proof-of-concept evaluation may be done at ANC, concurrently. These could include the following

operational functions, based upon the likely mandate of JTCs:-

- **Operations**. Joint Forces C2, joint fires, manoeuvre, sustainment and force protection functions will necessitate Joint Battlefield / Operational command centres.
- **Intelligence**. National intelligence sharing networks and databases, ISR fusion and tasking, enemy ORBAT, plans & Intentions.
- **Information Operations (IO).** Planning and execution to support the JTC's intent.
- **Space Operations / Functions**. C2 for space systems calls for unity of command. Dependence on space based systems is a vulnerability due to likely EW and redundancy in space-based C4ISR systems is a must. Space Coordinating Cells may be created at JTCs for coordinating force enhancement operations.
- **SF Operations**. Joint planning for reconnaissance and direct action by Special Forces and long range fires will need joint C4ISR.
- **EW**. Joint planning and coordination of ELINT, COMINT and EW will be necessary.
- **Cyber Operations**. Joint planning and execution of cyber defence and offence, in coordination with Defence Cyber Agency, is inescapable. Joint Cyber Cells, comprising of technology and language experts, may be operationalise at the JTCs.
- **Joint Sustainment**. Joint C4ISR capabilities for planning and execution of mobilisation, deployment, transportation and movement control, maintenance & service support, will be needed.

- **WMD**. CBRN detection, warning, defence and response frameworks will be needed.

Land Forces Related Joint C4ISR. Integration of the following land forced related C4ISR capabilities will be prudent:-

- **Joint Planning and Operations.** Joint land operation plan in support of the JTC's mission through a Joint Planning Group.
- **Intelligence.** Real time inputs to Joint Intelligence Centre/ Cell.
- **Air Operations.** Integrated Digital C2 frameworks for Advance HQ and JAAOC, akin to that established presently with Army Commands.
- **Joint Fires.** A Joint Fires/Targeting Coordination mechanism will be necessary.
- **Joint AB/HB, Transport and Lift Operations.** C4ISR for Joint planning and execution will be necessary.
- **Air Defence.** The proposed Joint AD Command (ADC), as and when created, will necessitate sharing and coordination of AD and Air Space Management (ASM) related C4ISR functions with JTCs during conflict/peace**.**
- **Civil-Military Cooperation.** C4ISR inputs for interagency coordination, specially for disaster management tasks, will be necessary, incase JTCs are given any administrative responsibilities in their AOR.

Air Force Related Joint C4ISR

Joint Air Operations**.** Development of a Joint Air Operations Plan to support the JTCs missions, based on the theatre course of action,

will necessitate creation of a JAOC alongside the JTC, under the AF Component Commander, also staffed by representatives of other components. This will enable planning and execution of the Air Tasking Order (ATO) and Close Air Support (CAS), Joint AD and ASM Plans, in concert with the Joint ADC, when established.

Maritime Related Joint C4ISR

MDA. Integrated MDA is already being shared Nationally though NC3I and Internationally though IFC-IOR. Integration with IACCS and Trigun needs to be prioritised.

Amphibious Operations. These are inherently joint operations and joint planning for surveillance, enemy maritime operations (aerial, surface, sub-surface), joint fires, HB, UAS and Counter UAS operations will be necessitated.

Joint C4ISR- The Pathways

Digitisation, Data Standardisation and Data Strategies

Information lies at the heart of C4ISR. To be leveraged as a weapon, it needs to be securely and shared across Services, intelligence agencies, and other stakeholders. This pre-supposes enterprise wide policies and strategies to regulate digitisation, and standardisation, especially for markup languages, dictionaries, metadata, waveforms, cloud services, cyber security and geo-spatial standards. A top down approach needs to be followed to regulate information management at the apex level, like the US, which recently promulgated a Digital Modernisation Strategy[54] encompassing cloud, artificial intelligence, C3 and cyber security, followed by a C3 Modernisation Strategy[55], to bridge the gap between legacy C3 capabilities and JADC2, while preserving current C3 capabilities and providing a seamless, resilient and secure C3 infrastructure. The US has also promulgated a Data

Strategy[56], which outlines principles, capabilities and 7 goals- Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable and Secure (VAULTIS), for becoming data-centric. The Digital India Vision was announced in 2015, followed by the Digital Vision of the Indian Army. The Services have formulated respective data Governance Policy. However, to preclude dissonance and disharmony in Service Strategies, which will adversely impact interoperability, cascading **Joint Strategies** need to be evolved, promulgated and strictly enforced, at the earliest, to make Joint C4ISR a reality. What we need are joint communications, data standards, interoperable systems and technologies that create a distributed, multi-domain C4ISR architecture. Two most important and urgent steps that need to be taken post haste are:-

- **Joint Intelligence & Geospatial ISR**. All the Services and National/State intelligence agencies generate an enormous amount of ISR data, essentially geospatial intelligence. The ongoing effort to sharing it in real time, across all stakeholders nationwide, both as a pull and a push model, should be expedited. Overtime, the system could mature into an operational and intelligence system. Most systems presently use Arc-GIS. There is a need to mandate interoperability with, or adoption of, the indigenous INDIGIS. ISTAR functions are inherently joint and it needs to be progressed as a Tri-Service project, instead of remaining a Single Service project, as at present.

- **Joint Cloud-based Storage and AI Based Analysis**. While the Services have adopted cloud-based strategies, the need of the hour is to leverage the information with AI to generate curated real time information from not just geospatial intelligence, but OSINT and ELINT. This is presently a stovepiped and duplicated single Service effort, which needs to be made a joint endeavour.

- **C4ISR for JTCs and Joint Functions**. Presently, the Services have Service-specific C4ISR Systems for facilitating SSA and DM needs of warfighting functions- C2, intelligence/information, manoeuvre, fires/ targeting, ELINT, EW, protection and sustainment. While proposed capabilities like Integrated Surveillance & Targeting System (ISAT-S) for mechanised/armoured formations[57] and UAVs for the infantry, are welcome steps at the tactical level, the Army needs to expedite IAIS operational and intelligence functionality, across all levels of command, failing which, its delayed integration with Joint C4ISR will seriously undermine any, and all efforts towards Joint C4ISR. As argued above, multiple single Service functions will have to be adapted in Joint C4ISR for the JTC model to fructify. Outlined below are ways to address two biggest impediments while designing C4ISR systems, Service-centric Cultures and Interoperability.

- **Addressing Cultural/ Procedural Barriers**. The desire to embrace integration and jointness, by addressing underlying siloed ethos and mindsets, must preferably come from all the stakeholders. The leap of faith taken on 1st Jan 2020 by appointing the first CDS with a mandate to usher path breaking changes within 3 years of appointment, has provided the foundation. It edifice must now be built by creating JTCs/Functional Commands, albeit incrementally, with due deliberation. Expeditious evolution and implementation of a 10 year Integrated Capability Development Plan, in consonance with the mandate of the CDS, through the proposed ICADS, should be the next big step. Joint C4ISR systems must figure high on the ICADS priorities. The following be kept in mind:-

    - Be driven by an apex level Joint Empowered

Interoperability Committee (JEIC). It must assess compliance with timelines and joint standards.

- Revamping legacy and stovepiped processes.
- Joint C4ISR systems will call for new joint organisations and processes, eg. for joint fires, joint ISR and autonomous systems.
- Allot commensurate financial and human resources.
- C4ISR systems could be evolutionary, developed in phases. The Users must articulate functional requirements, desired outcomes and standards. The requirements must not be revised midstream, which is a bane. Eg. the Army's foreclosed TCS and BSS, and re-tendered Akashteer.
- It is more important to field a workable system, learn from experimentation, evolve doctrines and TTPs eg. the Russians are believed to have high-end systems which the soldiers were not familiar with.
- Technical specifications could be defined in a manner that facilitates leveraging of disruptive innovations and exploitation of commercial technologies. Joint C4ISR projects should leverage the strengths of already fielded single service C4ISR systems and the lessons learnt.
- All Services must have a centre of excellence dealing with ICT, information and data science, for developing professionals and leaders conversant with C4ISR technologies. The services could create a specialised IT cadre, like the Navy, conversant with AI, big data and cyber security.

Interoperability.

- All C4ISR systems, Joint or Single Service, must comply with interoperability parameters, throughout their life cycle. Interoperability must graduate from being isolated, as presently, to pan-enterprise, since it bolsters flexibility and complementarity, especially during crisis responses.
- Trade-offs with other parameters like security, information overload, network traffic and vulnerability, must be assessed through actual tests, modelling and simulation (M&S), right from the feasibility stage.
- A spiral system development must be adopted, leveraging COTS technologies and open architecture, after carefully evaluating concomitant security risks.
- RFIs/RFPs for any new system or weapon, should be scrutinised for interoperability by the JEIC.
- Solutions must follow Security Development Operations (SecDevOps) approach.
- Standardised systems will usher transition from Service centric capabilities to networked, enterprise architectures that facilitate rapid integration of technologies. To cope with the challenges of standards and technology upgradation, countries follow modular open suite of standards, evolved by consortiums of government and industry[58]. For Joint C4ISR systems, there is a need to convey the commanders' intent and orders, unambiguously, through standardised data dictionaries and mark-up language.

Joint Communications Modernisation Strategies

Joint communication capabilities will ensure secure flow of information through shared cloud and AI enabled processing centres, to AI enabled joint decision nodes and effectors. Joint communications must ensure AI driven EMS capabilities, secure GPS/PNT signals and beyond line of sight (BLOS) communications. BLOS capabilities are inadequate for operations in denied and degraded communication environments, where HF SDR, with beam-forming antennae and wide-band technologies could be a good solution. The following actions are urgent and necessary:-

- **Small LEO Satellites**. With enhanced use of networked devices, even the dedicated defence communication satellites, which have been put to use since 2013, and the ones on the anvil, may fall short of future joint requirements. Small LEO satellitescan exponentially enhance defence C4ISR capabilities[59], as has been demonstrated by resilient Starlink NW in the Ukraine conflict. The costs and time should be factored.

- **Interoperability of Services Static Communications**. While all Services Networks have been awarded G4 security grade by SAG (DRDO), the Services do not trust inter-connections due to perceived vulnerability in the 'last mile' connectivity. Such issues must be resolved with compliance with insertion of appropriate bulk encryption units (BEU) or other feasible workarounds.

- **NFS and DCN**. Early operationalisation of the NFS project, which is nearing completion, expansion of DCN, and most importantly, exploitation of these systems for sharing operational, intelligence and sustenance information, in addition to the C4ISR for all joint functions envisaged for JTC/ Functional Commands, as elaborated earlier, is inescapable.

- **5G Infrastructure.** Accelerate development and deployment of military 5G infrastructure, especially in border areas.

- **Joint Tactical Networks (Interoperable SDRs)**. Going by the lessons of recent conflicts in Nagorno-Karabakh and Ukraine, it is evident that networks and nodes will be the most critical resource, since information is the main weapon. As mentioned earlier, the IN and IAF have already deployed SDRs and Army is in the process of accelerated deployment. Fielding a SDR based Joint TCS must be accelerated. DRDO built indigenous SDRs[60] should be trial evaluated expeditiously. A country specific operating environment called the India Software Communication Architecture (SCA) profile or Indian Radio Software Architecture (IRSA) is under development[61] by Department of Standardisation (DoS) and DRDO, together with academia and industry, in an early timeframe. It will enable Indian vendors to make SDRs inte roperable and security gradable. Another way to integrate all linked C2/ISR networks is the modular and scalable**, multi-data-link processor (DLP)** that can be customised by the end-user. When integrated with data links, the result is a network-centric expandable integration of data-links on naval, ground-based and airborne platforms[62].

- **Interoperability Bridges**. We need to innovate technological bridges to ensure interoperability between legacy C4ISR systems, without compromising their security and functionality. DARPA's networking and information programs such as DyNAMO, SHARE, SoSITE and STITCHES[63] have demonstrated these technologies that its program Mission Integrated Network Control (MINC) will need. It seeks to develop software that autonomously configures networks regardless of communication device or

networking resource, leveraging Software Defined Network (SDN) Technology. STITCHES is a software, designed to integrate heterogeneous systems by auto-generating low latency middleware between systems. It does not force a common interface standard, obviating the need to upgrade in order to interoperate[64]. We have already taken a nascent step[65].

- **Joint Aerial Layer Network (JALN) Concept.** To address network challenges, as a last resort, or even as a response to an urgent communication support for a Joint operation, a customised aerial platform can be used. The US has explored the concept of JALN airborne platforms[66], to augment capacity and connectivity, information sharing and NW management. In 2020, the US AF ordered a JALN High Capacity Backbone prototype[67], to be a critical enabler of JADC2. The US Army is also experimenting with aerial networks in degraded communication conditions, as part of its JADC2 project Convergence[68]. While being a cost intensive proposition with lesser viability in contested air spaces, the concept can be downscaled and exploited on UAVs, in areas with poor connectivity or in mission critical situations.

AI and Autonomous C4ISR Systems / Platforms. Transformation of C4ISR systems is not feasible without leveraging AI, big data and cloud computing. However, since connectivity may be challenging in contested environments, AI capabilities must enable the tactical edge, allowing them to connect at will, reducing EMS footprints. Swarms of drones with autonomy can perform complex C4ISR tasks collaboratively. Such collaborative C4ISR systems need edge computing. The Israelis have demonstrated the dividends of transforming kill-chains to kill-webs, powered by AI, during the conflict with Hamas in 2021.

Reviewing Doctrines, Concepts and Organisations

New Integrated and Joint Organisations. These will be required for Joint C4ISR. The multi-domain Russian Battalion Tactical Group (BTG), PLA's SSF elements, US military's ICEWS, Cyber Warfare Support Battalion and CEMA Teams are a few examples of ongoing experimentation in leading militaries. We could begin with integrating cyber and EW capabilities under a CEMA concept. Another idea worth examining is functional integration of EW and AD units in the Army to accelerate response and ensure protection and survivability, since AD and EW resources will be the first targets in Systems Warfare.

CAS. In Armies across the globe, Joint C2 is suboptimal for immediate/ emergency CAS, a very time critical function, despite embedded liaison teams like Air Control Teams (ACT) (comprising of GLOs and FACs), which uses voice communications links between the GLO (land forces), the FAC (an AF pilot on ground), and the pilot. IAF and Army functionaries at division/corps echelons reserve the right to veto the request. Experiences in conflicts across the globe have proved that this is a sub-optimal method, since radio links may be denied in a contested environment and static communications may be disrupted by strikes on communication centres / headquarters, which have significant EMS and visual signatures. Moreover, voice communications by pilots and ACT render both vulnerable. Air forces are now experimenting with low-detectable millimetric wave communications[69]. Since secure SDRs are now available, the answer lies in making the ACT an empowered Joint team with secure datalinks. This is especially important since the faultlines between IAF and Army will be certainly exploited by the adversaries. This gap has been bridged by deploying a Digitally Aided CAS (DACAS) system by the Turkish Air Force to enable the Turkish Joint Air Force Component[70].

ASM in the TBA. This too is an extremely important Joint function which is hostage to lack of interoperability between AF and Army C4ISR

systems for AD. The RASP is shared by IACCS up to the Corps/Division level, but will likely reach the forward based Air Direction/Control centres of the Army with avoidable latency, even if it is of the order of a few seconds. In order to obviate fratricide, the AF seeks its control to ensure freedom of operations in air, whereas the Army wishes to retain the freedom to engage hostile tracks to ensure force protection and deter the adversary. ASM, premised on the principle of centralised command and control, is apt for less contested and less hostile battlefield situations, where air superiority exists, even if temporarily. Considering the complex terrain and contested environments, the assumption of assured RASP to land forces may not hold true. This fragile inter-Service fault-line will also be exploited by the adversary to create fog, friction and indecision. The only solution, again, is to deliver the RASP to all control/direction centres in the forward areas through interoperable SDR communications with appropriate bandwidth. Even modern forces with interoperable AD C4ISR systems, advocate that C2 needs to be transformed by creating multi-functional, multi-Service teams, empowered to control/direct assets across the Services[71]. The organising principle should be to maximise the domains in which the Services can operate simultaneously[72]. The US is developing a program ACK (Adapting Cross Domain Kill-web) for AD commanders, which assists users in selection of sensors and effectors across domains (space, air, land, surface, sub-surface, EW and cyber), from all Services[73]. Communications across varied systems to enable this distributed fire control was done through the STITCHES bridge software, mentioned earlier in this paper. The organising principle of liaison/embedded teams is dated. Joint Multi-Domain C2 Teams can be the building blocks for C4ISR of any joint function, like deep fires, which entail coordinated use of airspace by strike aircraft, ground/sea-based missiles and artillery. Delegation of authority certainly entails risks, but infuses flexibility, and flatter, empowered C2 should be the organising principle for Joint organisations. The US Air Force,

as part of its recent Agile Combat Employment concept, tailored for contested environments, is leveraging the Army and Marine Corps ability to establish short-duration Air Traffic Services (ATS), through ATS companies in aviation brigades, which operate the ATNAVICS System to control both rotary-wing and fixed-wing assets. This structure provides flexibility to support the joint force at the tactical level through joint all domain and ACE concept[74]. The Turkish system also includes ATO, ASM and a single integrated air picture is shared digitally in real time with all C2 elements[75]. These concepts must be trial evaluated with modelling and simulations (M&S) and war-games/exercises, to formalise joint concepts and TTPs. The answer lies in integrating IACCS, Trigun and Akashteer, since technology is not an impediment**.** RASP needs to be shared on a data-link with Army Aviation assets, integrating ever increasing unmanned assets.

War-Gaming, M&S and Exercises

M&S and experimentation of Joint C4ISR systems, will facilitate tradeoffs with other competing capability development programs. The US Air Force repelled a Chinese invasion of Taiwan during a war-game by featuring many yet to be developed technologies and concepts[76]. In similar war games held earlier, it had failed disastrously. Such war-games offer an insight into what mix of capabilities are needed in future scenarios. For example, it assumed that the Air Force had fielded its ABMS, interoperable with the Navy's Project Overmatch and the Army's Project Convergence, which are all under development. Instead of separate command/liaison organisations for the land, maritime and air domains, the Air Force created small Joint C2 teams, of five to 30 individuals from all the Services. These empowered C2 teams executed operations using portable tablets, and were thus mobile and survivable with low signatures, in contrast with C2 nodes with bigger signatures. Such war-games must also form part of our ICADS process for prioritising tri-service capabilities.

R&D and Innovation

Though 15 out of 75 AI-powered defence products launched in July 2022 were related to C4ISR, funding for R&D to DRDO and defence innovation initiatives like iDEX has only partially incentivised experimentation and risk-acceptance. Partnerships with IITs and other centres of excellence need to be bolstered.

Conclusion

Plans rarely survive the first contact with the adversary and have to be reviewed dynamically, based on SSA, whether on the move or static. Agile, integrated, joint and distributed warfighting entities need fast and resilient joint OODA, trumping that of the adversary. Joint C4ISR enables collaborative decision making at all levels, under conditions of cognitive fog, friction and uncertainty, leveraging inter-service, multi-domain and multi-agency capabilities. We have the building blocks in place and with the operationalisation of NFS shortly, a joint communication backhaul will be available. Indigenous joint SDRs under trials/development can enable Joint C4ISR at the tactical level, transforming critical joint functions like joint fires, CAS, integrated ADS and ASM. However, we must field these soonest, since evolution of new joint organisations, doctrines and concepts across domains takes considerable time. If any proof is needed, the ineptitude and failure of the Russian Joint forces in Ukraine provides instructive lessons. Joint C4ISR systems must not wait for JTCs- the form will follow function.

A detailed and unbiased cost-benefit analysis of C4ISR systems is equally important. They must deliver force effectiveness by contributing to outcomes in physical, information and cognitive domains. While better DM, real time SSA and communications cannot substitute mass and firepower, they are inescapable force multipliers. Trade-offs with competing Tri-Service capabilities, leveraging the ICADS process and

wargaming would be pragmatic. The major barrier to joint C2 structures and Joint C4ISR, are the stovepiped Service cultures, and not technology. The pathways outlined are achievable, all we need is a joint resolve to set, and achieve, the milestones.

***Lt Gen Sunil Srivastava, AVSM, VSM** (Retd)** is a former Commandant of the OTA Gaya and is presently, Director Centre for Joint Warfare Studies (CENJOWS), New Delhi.

Endnotes

1 James Black, et al 2022, "Multi-Domain Integration in Defence Conceptual Approaches and Lessons from Russia, China, Iran and North Korea", RAND Corporation, Santa Monica, Calif., and Cambridge, UK; https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1048606/RAND_RRA528-1.pdf, accessed on 10 July 2022

2 Ibid

3 Ibid

4 Ibid

5 Roger McDermott, Moscow Showcases Breakthrough in Automated Command and Control, Eurasia Daily Monitor Volume: 16 Issue: 164, November 20, 2019; https://jamestown.org/program/moscow-showcases-breakthrough-in-automated-command-and-control/, accessed on 10 July 2022

6 Ibid

7 Anna Nadibaidze, "Russian Perceptions of Military AI, Automation and Autonomy", The Foreign Policy Research Institute, Jan 2022; https://www.fpri.org/wp-content/uploads/2022/01/012622-russia-ai-.pdf, accessed on 10 July 2022

8 Ibid

9 Kevin Pollpeter, 2010 "Towards an Integrative C4ISR System: Informationization and Joint Operations in the Peoples Liberation Army", https://www.jstor.org/stable/pdf/resrep11945.8.pdf, accessed 10 July 2022

10 Ryan Fedasiuk, Jennifer Melot and Ben Murphy, "Harnessed Lightning- How the Chinese Military is adopting Artificial Intelligence", Center for Security and Emerging Technology, Oct 2021, https://creativecommons.org/licenses/by-nc/4.0/cset.georgetown.edu, accessed 17 July 2022

11 US Department of Defence, 'DoD Announces Release of JADC2 Implementation Plan', 17 March 2022, https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/, accessed 17 July 2022

12 Ibid

13 Congressional Research Service, 'Joint All-Domain Command and Control (JADC2)', updated Jan 2022, https://sgp.fas.org/crs/natsec/IF11493.pdf/, accessed 17 July 2022

14 David L Rockwell, 'US Army's Warfighter Information Network-Tactical (WIN-T)' January 2020, https://www.tealgroup.com/index.php/teal-group-media-news-briefs-2/teal-group-news-media/item/us-army-s-warfighter-information-network-tactical-win-t, accessed 17 July 2022

15 Dan Ward, 'JTRS: A Cautionary Tale for Today', MITRE AiDA, 01 April, 2020, https://aida.mitre.org/blog/2020/04/01/jtrs-a-cautionary-tale-for-today/, accessed 17 July 2022

16 Ron Miller, 'Pentagon announces new cloud initiative to replace ill-fated JEDI contract', 20 Nov 2021, https://techcrunch.com/2021/11/19/pentagon-announces-new-cloud-initiative-to-replace-ill-fated-jedi-contract/, accessed 17 July 2022

17 Indian Defence News, 'Aero India 2019: An Israeli Data Link For IAF', http://www.indiandefensenews.in/2019/02/aero-india-2019-israeli-data-link-for.html, accessed 24 July 2022

18 WIONEWS, February 2020'IAF has to Reorient, Retrain to Changed War Paradigm: Dhanoa', https://www.wionews.com/india-news/iaf-has-to-reorient-retrain-to-changed-war-paradigm-dhanoa-279615, accessed 24 July 2022

19 Anil Chopra, 'Towards an Integrated Military Future' September 2021, Raksha Anirveda, https://raksha-anirveda.com/towards-an-integrated-military-future/, accessed 24 July 2022

20 Himadri Das, 'Maritime Domain Awareness in India: Shifting Paradigms' May 2021, https://www.maritimeindia.org/maritime-domain-awareness-in-india-shifting-paradigms/, accessed 24 July 2022

21 Ibid

22 Ibid

23 PC Katoch, 'Indian Army's Tactical Communications Programme', May 2019 https://www.pressreader.com/india/sps-landforces/20190510/281505047645511/, accessed 24 July 2022

24 Anil Chopra, op cit

25 PC Katoch, 'Indian Army's Tactical Communications Programme', May 2019, https://www.pressreader.com/india/sps-landforces/20190510/281505047645511/, accessed 24 July 2022

26 Press Information Bureau, Government Of India, 'Mobile Integrated Network Terminal For Indian Army Under Atmanirbhar Bharat Abhiyaan', March 2021, https://www. pig.gov.in/Pressreleaseshare.aspx?PRID=1704393, accessed 24 July 2022

27 Prakash Katoch, 'Battlefield Management System for the Army-Where Are we?', December 2017, https://strategicfront.org/forums/threads/battlefield-management-system-for-indian-army-where-are-we.395/, accessed 24 July 2022

28 Shilpi Chakravarty, 'Geospatial a Crucial Component of the Indian Army- Lt Gen Anil Kapoor Director General Information Systems', 19 April 2018, https://www.geospatialworld.net/article/geospatial-crucial-component-indian-army/, accessed 24 July 2022

29 'INDIGIS: An Indigenous GIS for Defence Applications', Technology Focus, Vol 30, Issue I, Feb 2022, ISSN 0971-4413, https://www.drdo.gov.in/TF_Feb2022_0.pdf/, accessed 24 July 2022

30 Technology Focus, Futuristic Airborne Surveillance Technologies, 'Audio and Data Management System', Vol 29, Issue 3, June 2021, ISSN 0971-4413, https://www.drdo.gov.in/TF_Jun2021_0.pdf/, accessed 24 July 2022

31 Technology Focus, Futuristic Airborne Surveillance Technologies, 'Intelligence, Surveillance, Targeting and Reconnaissance' Vol 29, Issue 3, June 2021, ISSN 0971-4413, https://www.drdo.gov.in/TF_Jun2021_0.pdf/, accessed 24 July 2022

32 AK Sachdev, “C4ISR and Autonomous Capabilities”, Indian Defence Review, Issue Vol. 36.4, Oct-Dec 2021 | Date: 04 Jan 2022; http://www.indiandefencereview.com/news/c4isr-and-autonomous-capabilities/, accessed 24 July 2022

33 The Joint Indian Armed Forces Doctrine, Directorate of Doctrine, Doctrine Operations and Training Branch, Headquarters Integrated Defence Staff, New Delhi, Second Edition April 2017.

34 Joint Doctrine For Air-Land Operations, Headquarters Integrated Defence Staff Ministry Of Defence, March 2010

35 AK Sachdev, op. cit

36 Ibid

37 V K Saxena, ‘Air Defence Command – A Bold Initiative’, March 2021, https://chanakyaforum.com/air-defence-command-a-bold-initiative/, accessed 24 July 2022

38 Harsha Kakkar, Disagreements On Theatre Commands: India Needs This Project; Don’t Dump It As Unnecessary”, 31 July 2022, https://www.firstpost.com/opinion/disagreements-on-theatre-commands-india-needs-this-project-dont-dump-it-as-unnecessary-10986471.html, accessed 31 July 2022

39 Ramesh Rai, “Divide And Diminish: Joint Air Defence Command Is An Operationally Unviable Idea”, https://forceindia.net/guest-column/divide-and-diminish/, accessed 24 July 2022

40 Diptendu Choudhury, July 2020 ‘Air Defence is Everywhere’, Vivekanand International Forum, 24 July 2020, https://www.vifindia.org/article/2020/july/24/air-defence-is-everywhere/, accessed 24 July 2022

41 North American Aerospace Defense Command, https://www.Nora.mil/About-NORAD/, accessed 24 July 2022

42 Theatre Air Control System, Air Force Doctrine Publication 3-03, Counter Land Operations, updated October 2020, https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-03/3-03-D23-TACS.pdf, accessed 24 July 2022

43 Fredrik Westerlund and Susanne Oxenstierna (eds), “Russian Military Capability in a Ten-Year Perspective – 2019”, FOI ISSN 1650-1942, https://www.academia.edu/41325809/2019_Russian_Military_Capability_in_a_Ten_Year_Perspective, accessed 24 July 2022

44 Nicholas Myers, ‘The Russian Aerospace Force’, 2018, https://wsb.edu.pl/files/pages/634/8-3.pdf, p 97, accessed 24 July 2022

45 Justin Bronk, “Modern Russian and Chinese Integrated Air Defence Systems : The Nature of the Threat, Growth Trajectory and Western Options, Royal United Services Institute, Jan 2020, https://static.rusi.org/20191118_iads_bronk_web_final.pdf; p 12, accessed 24 July 2022

46 China Aerospace Studies Institute, ‘PLA Aerospace Power: A Primer on Trends in China’s Military Air, Space, and Missile Forces’ 3rd Edition; https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2022-08-15%20PLA%20Primer%203rd%20edition.pdf; p 16, accessed 24 July 2022

47 Ibid pp 31-32

48 Bronk op cit, n13

49 Kenneth W Allen and Christina L Garafola, ’70 Years of the PLA Air Force’, China Aerospace Study Institute, April 2021, pp 109-110; https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/PLAAF/2021-04-12%20CASI_70%20Years%20of%20the%20PLAAF_FINAL%20ALL.pdf, accessed 24 July 2022

50 Wang Mingqian & Cao Shuai, “A survey on C4ISR system architecture technique”, Global Journal of Engineering and Technology Advances, 2020, 02(03), 054–066, https://doi.org/10.30574/gjeta.2020.2.3.0019, accessed 24 July 2022

51 National Academies of Sciences, Engineering, and Medicine, ‘Realizing the Potential of C4I: Fundamental Challenges’, Washington, DC: The National Academies Press, 1999 https://doi.org/10.17226/6457, accessed 30 July 2022

52 Ibid

53 Press Information Bureau, Semiconductor Chip Designing and Manufacturing, 06 April 2022, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1814029, accessed 30 July 2022

54 US Department of Defense Directive 5144.02, September 2017, ‘DoD Chief Information Officer’ https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/514402p.pdf, accessed 30 July 2022

55 US DoD C3 Modernisation Strategy, September 2020, accessed at https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf, accessed 30 July 2022

56 Executive Summary, DoD Data Strategy, September 2020, https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF, accessed 30 July 2022

57 Amrita Nayak Dutta, ‘Infantry Combat Vehicles In, Soviet-Era BMP-2 Out: How Army Plans to Modernise Mechanised Infantry’, 27 Aug 2022, https://www.news18.com/news/india/infantry-combat-vehicles-in-soviet-era-bmp-2-out-how-army-plans-to-modernise-mechanised-infantry-5832541.html, accessed 28 Aug 2022

58 Nathan Strout, ‘SOSA Consortium Unveils First Standards for Military Sensor Technologies’, October 2021, Defense News, https://www.defensenews.com/digital-show-dailies/ausa/2021/10/11/sosa-consortium-unveils-first-standards-for-military-sensor-technologies/ accessed 06 August 2022

59 Kartik Bommakanti, ‘Strengthening the C4ISR capabilities of India’s Armed Forces: The Role of Small Satellites’, Observer Research Forum, 15 June 2020, https://www.orfonline.org/research/strengthening-the-c4isr-capabilities-of-indias-armed-forces-the-role-of-small-satellites-67842/, accessed 6 Aug 2022

60 KNN Bureau, ’DRDO Built Indigenous SDRs to Help Achieve Self-Reliance In Field of Secured Radio Communication’, 26 July 2022, https://knnindia.co.in/news/newsdetails/sectors/drdo-built-indigenous-sdrs-to-help-achieve-self-reliance-in-field-of-secured-radio-communication/, accessed 6 Aug 2022

61 Manjeet Negi, ‘Defence ministry fast-tracks indigenisation of Software Defined Radios for Armed Forces, 27 July 2022, https://www.indiatoday.in/india/story/defence-ministry-fast-tracks-indigenisation-of-software-defined-radios-for-armed-forces-1980351-2022-07-27, accessed 6 Aug 2022

62 Prasun K Sengupta, ‘Integrated Approach’, https://forceindia.net/defexpo-2020/integrated-approach-prasun-k-sengupta/, accessed 6 Aug 2022

63 “DARPA Seeks “Always On” Interconnected Networks for Multidomain Missions”, Defense Advanced Research Projects Agency, May 2021; https://www.darpa.mil/news-events/2021-05-07, accessed 6 Aug 2022

64 “Creating Cross-Domain Kill Webs in Real Time”, Aerospace and Defence News, 18 Sep 2020, https://www.asdnews.com/news/defense/2020/09/18/creating-crossdomain-kill-webs-real-time, accessed 6 Aug 2022

65 Chakravarty, n. 28, P (U)

66 Joint Concept for Command and Control of the Joint Aerial Layer Network, 20 March 2015, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_aerial_layer_network.pdf?ver=2017-12-28-162026-103, accessed 7 Aug 2022

67 'Cubic Awarded Contract to Demonstrate High Capacity Backbone System for US Air Force', 3 Aug 2020, https://www.cubic.com/news-events/news/cubic-awarded-contract-demonstrate-high-capacity-backbone-system-us-air-force#:~:text=Cubic%20is%20a%20technology%2Ddriven,militaries%27%20effectiveness%20and%20operational%20readiness, accessed 7 Aug 2022

68 Colin Demarest, US Army Reaches for the Sky to Solve Communication Needs, 21 June 2022, https://www.c4isrnet.com/battlefield-tech/it-networks/2022/06/21/us-army-reaches-for-the-sky-to-solve-communication-needs/#:~:text=WASHINGTON%20%E2%80%94%20Those%20with%20boots%20on,on%20battlefields%20the%20world%20over, accessed 7 Aug 2022

69 Thomas Whittington, 'Stealthy Airborne Communications', European Security and Defence, July 2022, ISSN 1617-7983, accessed 7 Aug 2022

70 Osman Aksu, 'Close Air Support Command and Control: Digitally Enhanced CAS Operations', Joint Air Power Competence Centre, July 2022, https://www.japcc.org/journals/journal-edition-34/, accessed 7 Aug 2022

71 Leland Cowie, Todd Graff, Craig Cude, and Brad Dewees, "To Build Joint Command and Control, First Break Joint Command and Control", War on The Rocks, 2 July 2021, https://warontherocks.com/2021/07/to-build-joint-command-and-control-first-break-joint-command-and-control/, accessed 13 Aug 2022

72 Ibid

73 "Creating Cross-Domain Kill Webs in Real Time", Aerospace and Defence News, 18 Sep 2020, https://www.asdnews.com/news/defense/2020/09/18/creating-crossdomain-kill-webs-real-time, accessed 13 Aug 2022

74 Matthew Arrol, 'The Key To Maximizing The Air Force's Agile Combat Employment Concept? The Army', Modern War Institute, 28 June 2022, https://mwi.usma.edu/the-key-to-maximizing-the-air-forces-agile-combat-employment-concept-the-army/, accessed 13 Aug 2022

75 N.69

76 Valerie Insinna, "A US Air Force war game shows what the service needs to hold off - or win against - China in 2030", 12 April 2021, Defense News, https://www.defensenews.com/training-sim/2021/04/12/a-us-air-force-war-game-shows-what-the-service-needs-to-hold-off-or-win-against-china-in-2030/, accessed 14 Aug 2022

REDEFINING C4ISR & ADAPTIVE EVOLUTION OF DIGITAL INTELLIGENCE

Wg Cdr Srambikal Sudhakaran (Retd)*

C2 (Command & Control) is at the very foundation of **C4ISR**. War is a very complex affair and since there is no concept of being second in the game, every aspect of planning and execution is expected to be flawless in every which way. The term "Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance" (C4ISR) was coined by the U.S. Department of Defense (USDoD) as a more current and automation-focused derivation of the standardized military term "Command and Control" (C2), which broadly refers to attributes and systems that provide problem-solving resources to carry out missions. Most nations employ some form of C2 military structure, but a fully operational C4ISR structure encompasses more advanced and more expensive – technologies, assets, and capabilities.

The main motivation behind the conceptualization of the C4ISR framework was to "**See through the Fog of War**" and bring in **clarity** and a **sense of assuredness** alongwith **surety to the battlefront**. The Information age of the last century did evolve this framework to a broader one by upgrading it to **C5ISR & C6ISR**. While **Cyber-defense** was the 5th C, **Combat systems** was the 6th C. this definition of C6ISR still woefully falls short of embracing the actual ground realities of modern warfare.

The C4ISR framework was coined at a time when the advanced military powers were fighting under the broader concept of **Net-centricity of Warfare (NCW).** The components of C4ISR therefore

were restricted to communication between computers to ensure command and control by delivering real-time information obtained through Reconnaissance & Surveillance. The aspect of Cyber-defense was accommodated when it was realized that there was a threat to the reliability & quality of information. When the volume of information became too big to handle in real-time, advanced automated systems took over the job of decision making & complex calculations to present to the decision makers the various possibilities to deploy and optimize their fire capabilities.

Take for example the ongoing Russian-Ukraine conflict. While it is a matter of public knowledge that the war is being fought by NATO & Russia, with US being the actual face of NATO and Russia fighting with clandestine support from its main ally China. In a sense this a unique war, where multiple wars are being fought between different countries in different domain. A layered warfare spreading across geographies & domains fought primarily with information as the main weapon. The most notable aspect of this war is that, this is the first war with some level of AI having crept into the OODA loop. The C2 family of framework still has not adapted to this modern dimension of technology led Intelligence enabled warfare. This is what we need to make explicit in our discourse on C4ISR. “Command Control Communications Computers Intelligence Surveillance and Reconnaissance” is meaningless in itself as a descriptive amalgam.

The advent of AI due to the enhanced processing ability & miniaturization of compute nodes, has led to the evolution of the concept of net centricity of warfare. Today connectedness of a system is basic pre requisite and considered mundane. The superiority of the force & metrics of success lies in its ability to take agile decisions in dynamic situations across battlefront, while ensuring minimal loss of human lives. This requires a higher degree of autonomous freedom for the digital systems as any human in the loop can significantly slow down the agility of the process

consequently defeating the very purpose of having such systems. The pre-requisite for such autonomous operation is the trust on the dependability & reliability of such decision-making process. Though a full-fledged autonomous system is still a decade away before seeing the actual battlefield, it is definitely the path to tread as far as C2 family of frameworks are concerned. It is under this backdrop that **we need to redefine the concept of C4-C5-C6 family of ISRs to a new framework which can accommodate the crucial aspect of Digital Intelligence in Military Decision Support systems.**

Command & Control shall always be the end result of whatever new framework that is coined today or in the near future. The major change has happened in the field of Communications, Computers, Cyber & Information. This has led to a generational change as far as surveillance and Reconnaissance is concerned. The next few decades will see a hybrid model of intelligence in the decision-making process. i.e., Intelligence of Humans augmented with Intelligence of Digital systems.

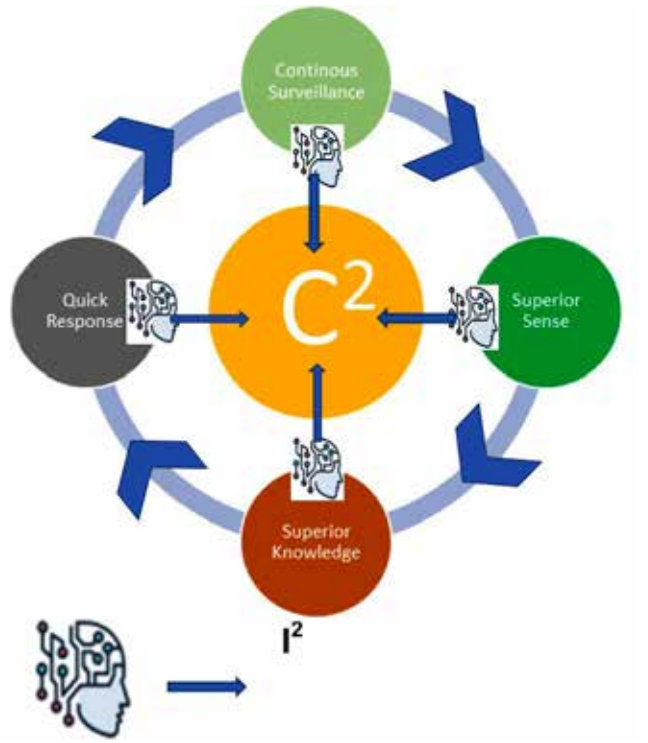
The term Intelligence as opposed to Information has a much broader connotation & consequence. Intelligence essentially means “the skilled use of Reason”. In this context the broader term **intelligence therefore encapsulates “Information, Surveillance and Reconnaissance”** to generate a set of rationale that is transformed into actionable commands. The Next generation of Intelligence enabled warfare (**IEW)** would therefore exercise Command & Control through two forms of Intelligence (Human& Machines). The term C2I2 systems therefore shall be a more practical terminology for the Military decision support framework which shall ensure seamless delivery of information flow to enhanced battlefield awareness while ensuring informed decision making. **C2I2 systems aim at enhancing our own OODA loop by acceleration of the decision-making loop, with superior information dissemination and information quality that reduce “friction of war” and “lift the fog of war.”** The exploitation of “C4” collectively by the broader “I^2” as

an enabler overcomes the traditional time-and-space barriers imposed on communications & computational systems and generates a shared awareness that is able to reduce the “friction of war”.

Generation of operational knowledge seeks to establish “information superiority” for the fighting force as a whole, and serves to militate against the perennial “fog and friction of war”. This Knowledge generation when done without any possibility of Bias, vested interest or possibility of compromise by the adversary, will prove to be the perfect anti dote to any trying situations that emerge in the battlefield. It is often said that “Air Superiority” & “Space Superiority” are key aspects to hold power on land. In the modern era “Information superiority” is far more vital for achieving Air superiority and Space superiority. Russia’s inability to declare victory despite being a statistically superior force is a live testimony to this fact. Information superiority can only be achieved by a superior intelligence platform.

When we refer to **Intelligence platform, we must also look at the concept of Intelligence holistically and at par with human intelligence in terms of its versatility & creativity**. Such systems therefore can unleash the possibility of engineering decision support platforms far beyond the capability of human minds. This is how superior platforms could come into existence at breakneck speeds which could throw in the element of surprise in a battlefield and significantly alter the consequences.

The next gen C2 framework are therefore expected to deliver commands to battlefronts seamlessly with the desired level of accuracy and speed. **Agility with adequate Quality is therefore important to exercise Command & Control in the age of Intelligent enabled warfare.** While the previous century saw radio waves bringing in the speed of light to the communication domain, this century shall be about acceleration of decision making with digital systems at comparable speeds. To achieve



this the C2 framework needs to evolve & accommodate technology frameworks in the domain of Digital Intelligence to stay relevant.

***Wg Cdr Srambikal Sudhakaran (Retd),** is a CEO Qu Gates Technologies.

GEOSPATIAL AND DATA FUSION TECHNOLOGIES FOR REAL TIME SITUATION AWARENESS AND DECISION MAKING

Brigadier (Dr) Rajeev Bhutani (Retd)*

Abstract

A modern C4ISTAR (Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition and Reconnaissance) System requires ***real time situation awareness,*** *derived from appropriate sensor data. The sensors must be geo-referenced with timing accuracy by using geospatial technologies and the sensors data must be fused in such a way that at the right time, the right piece of high-quality information relevant to a given situation is transmitted to the right user and appropriately presented. Only then can the data support* ***goal-oriented decision making*** *at all levels of decision hierarchy.*

By aggregating, organising, fusing & processing intelligence from multiple systems such as multispectral sensors, Synthetic Aperture Radar (SAR), optical, thermal, and geophysical sensors, Light Detection and Ranging (LiDAR), Geographic Information System (GIS) and Global Positioning System (GPS), also known as Geolocation systems, Common Operating Picture (COP) with relevant, accurate and timely intelligence is build up that can be used by decision makers for handling the threats efficiently and effectively.

Geospatial technologies were used fruitfully to establish the location of

*Russian troops and equipment against Ukraine in 2014. However, that had been categorised under **Digital forensic techniques.** In order to make these technologies as a component of C4ISTAR, these have to be fused with multi-domain, multi-sensor data obtained from varied sources so as to produce near-real-time situation awareness. C4ISTAR based on Geospatial and data fusion technology will act as a Force-Multiplier, providing multitudinous advantage over the enemy.*

Introduction

Although situation awareness is needed for many domains such as emergency/ disaster response, infrastructure monitoring etc., but it is extremely important for Armed Forces and in particular for Air Force. Situation awareness has been an integral part of military command and control (C2). Due to advent of modern technologies, ambit of C2 is now vastly enhanced to encompass C4ISTAR Systems. This acronym denotes computer-assisted functions for C4 (Command, Control, Communications, Computers), I (Intelligence), and STAR (Surveillance, Target Acquisition and Reconnaissance) in order to enable the coordination of defence-related operations. C4ISTAR systems aim at information dominance over potential opponents. Basic component of C4ISTAR, modular and flexibly designed as “systems of systems”, is the combination of sensor systems and data bases with appropriate sensor data and information fusion sub-systems.[1]

The commanders at all levels of hierarchy as well as automated decision making systems have access to vast amounts of data. In order to optimize use of this high degree of data availability for various decision tasks, the continuous streaming of data should not overwhelm the human beings as also decision making machines involved. On the contrary, the data must be fused in such a way that at the right time, the right piece of high-quality information relevant to a given situation is transmitted to the right user and appropriately presented or in other words, requirement is

to have **real time situation awareness.** Only then can the data support **goal-oriented decision making** at all levels of decision hierarchy.

The modern development of **sensor data fusion systems** has been made possible over the recent decades by substantial progress in these areas: **Advanced and robust sensor systems**; Communication links with sufficient bandwidths; Information technology for dealing with large data streams; Technical interoperability to build distributed “systems of systems” for sensor exploration and data exploitation; Mature navigation systems i.e., **Geospatial technologies** for providing common frames of reference for the sensor data based on precise space-time registration; and Advanced and ergonomically efficient Human-Machine Interaction (HMI) tools as an integral part of man-machine-systems presenting the results of sensor data fusion systems to the users in an appropriate way.[2]

An overview of ‘real time situation awareness’ required from armed forces perspective is pictorially depicted at Figure 1 below:-

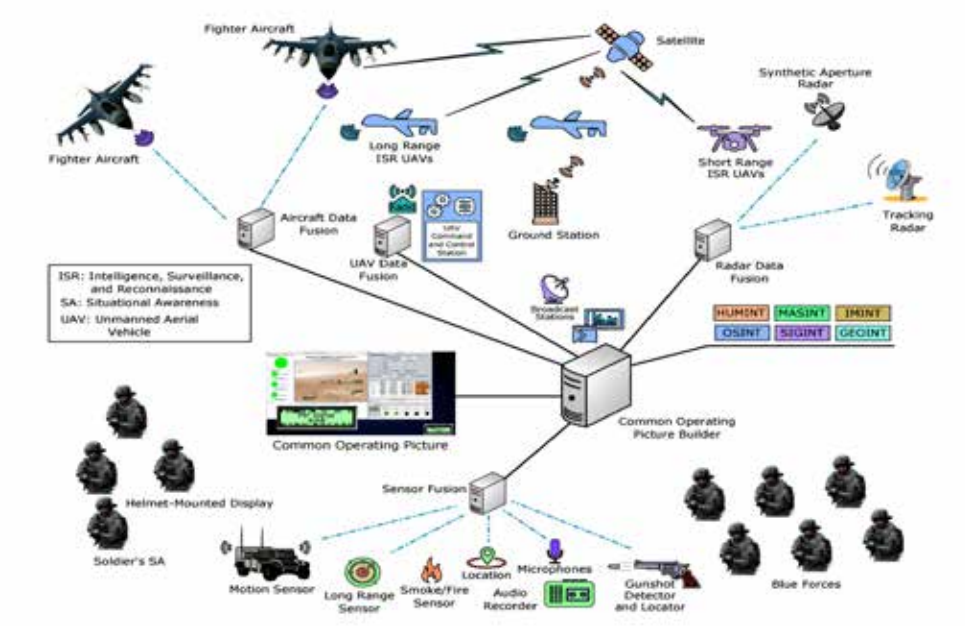


Figure 1: An Overview of Real Time Situation Awareness - Armed Forces Perspective (Source: Arslan Munir et al., Situational Awareness: Techniques, Challenges, and Prospects)[3]

The subject is being studied under the following heads:-

- Definition of Terms.
- A Model for Real Time Situation Awareness and Dynamic Decision-Making.
- Technologies Required for Situation Awareness.
- Utilisation of Geospatial and Data Fusion in the Indian Armed Forces.

Definition of Terms

Geospatial Technologies. It is a term used to describe the range of modern tools contributing to the geographic mapping and analysis of the Earth and human societies.[4] Geospatial technology enables us to acquire data that is referenced to the earth and use it for analysis, modeling, simulations, and visualization. The basic list of Geospatial technologies encompasses Remote Sensing (**RS**), Geographic Information System (**GIS**) and Global Positioning System (**GPS**).[5]

Data Fusion. It refers to combining data from multiple sources to improve the potential values and interpretation performances of the source data, and to produce a high-quality visible representation of the data. Fusion techniques are useful for a variety of applications, ranging from object detection, recognition, identification and classification, to object tracking, change detection, decision making, etc.[6]

The concept of data fusion is not limited to the fusion of data from different sources. A change analysis that occurs on the same type of spatial data over a period of time (multi-temporal data) can also be considered a

form of spatial data fusion but in this case the fusion component is in time.[7]

Remote Sensing Data Fusion. It is one of the most commonly used techniques, aims to integrate the information acquired with different spatial and spectral resolutions from sensors mounted on satellites, aircraft and ground platforms to produce fused data that contains more detailed information than each of the sources.[8]

Situation Awareness (SA). Situation awareness is formally defined as "the perception of the elements in the environment within a volume of time and space, comprehension of their meaning and the projection of their status in the near future".[9]

SA (Armed Forces Perspective). SA refers to the capability to conceive the current and future disposition of friendly and enemy's aircraft and surface threats within a volume of space. SA comprises of three distinct stages or levels: perception, comprehension, and projection.[10]

A Model for Real Time Situation Awareness and Dynamic Decision-Making

Companies like Rolta and Mistral have developed C2 solutions, for connecting and managing disparate technologies, like variety of sensors including radars, GPS tracking, GIS mapping, and life critical systems. By aggregating, organising, fusing & processing intelligence from these systems, it builds Common Operating Picture (COP) with relevant, accurate and timely intelligence that can be used by decision makers for handling the threats efficiently and effectively. Following an alert, alarm, or event, the system provides multiple options, such as Notifications, escalations, or response plans to respond to a situation.[11] These systems are very useful for meeting the requirements of Homeland security or Emergency / Disaster response.

However, in the fast moving battle like air combat engagements, desired function of SA is for tracking the enemy's aircraft current move and predicting its future action, a fraction of seconds before the enemy himself observes his own aircraft's movement. SA can also be viewed as equivalent to "observe" and "orient" phases of the observe-orient-decide-act (OODA) loop. Since in the aerospace, pilots have to deal with many arduous situations such as: higher levels of aviation traffic, inclement weather (e.g., storms, fog), recently unmanned aerial vehicles (UAVs) in the air space, and locating and engaging the targets on ground; they need to be equipped with an advanced real time SA system to cope with these antagonistic conditions and provide dynamic decision-making.[12]

The information processing approach has been best represented by M. R. Endsley's (1995) theoretical three level model of situational awareness.[13] Situation Awareness and dynamic decision-making model shown in Figure 2 below has been adopted from Endsley's concept:-

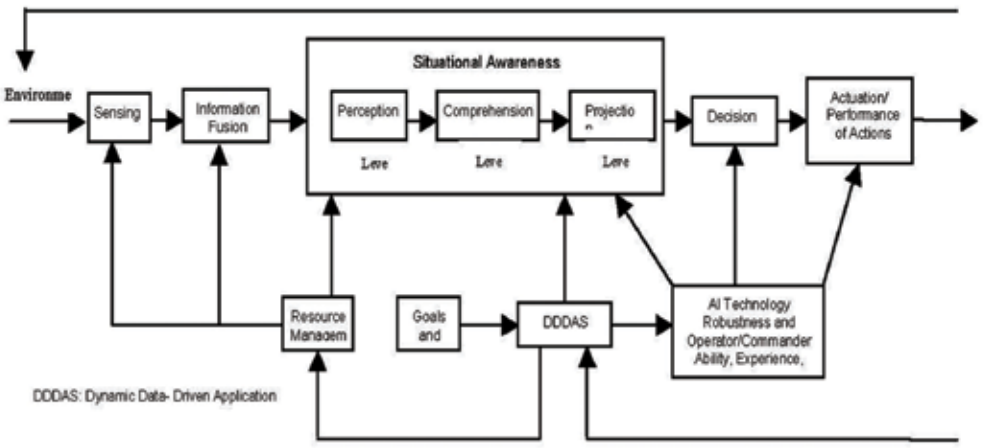


Figure 2: Situation Awareness and Dynamic Decision-Making Model (Source: Source: Arslan Munir et al., Situational Awareness: Techniques, Challenges, and Prospects)[14]

The model has an **SA core** whereas **sensing and decision-making elements** are built around the SA core. A multitude of sensors sense the environment to acquire the state of the environment. The sensed information is fused together to remove the redundancies in the sensed data, such as multiple similar views captured by different cameras or quantities sensed by different sensors in close locality, and also to overcome the shortcomings of data acquired from a single source, such as occlusions or change in ambient lighting conditions.[15] The fused data is then passed to the SA core, which comprises of three levels or stages:-

- **Perception – Stage 1 SA.** The first stage of acquiring SA is the perception of the status, attributes, and dynamics of the relevant elements in the surroundings. For example, a pilot needs to discern important entities in the environment such as other aircraft, UAVs, terrain, ground targets, and warning lights along with their relevant characteristics.[16]

- **Comprehension – Stage 2 SA.** The second stage of SA is the comprehension of the situation, which entails understanding the entities (acquired in Stage 1) and integrating them together, in relation to the operator's objectives. For instance, a pilot must understand the significance of the perceived elements in relation to each other.

- **Projection - Stage 3 SA.** The third stage of SA is prediction or estimation of the status of entities in the surroundings in future, at least in the near future. For example, from the perceived and comprehended information, the experienced pilots/operators predict possible future events (Stage 3 SA), which provides them knowledge and time to determine the most befitting course of action to achieve their objectives.[17]

The SA core also receives input from the commanders at strategic or operational levels, which can be supplemented by artificial intelligence (AI)

assisted decision-making. Perception is organised through the standard information fusion and resource management loop. However, to better manage the resources according to changing situations, a dynamic data-driven application systems (DDDAS) module is established to provide input to the resource management module, which in turn manages the sensors sensing the environment and computing resources in the SA core. In the DDDAS module, the computation and instrumentation facets of an application system are dynamically assimilated in a feedback control loop such that the instrumentation data can be dynamically fused into the executing model of the application. The executing model can in turn control the instrumentation. The DDDAS module can help guide and reconfigure sensors to increase the information content of the sensed data for enhancing SA of the activities of interest in the environment.[18]

Due to the recent advancements in AI, AI has become an integral part of SA core and dynamic decision-making. AI assists operators/pilots in comprehending the situation (Stage 2 SA) and then making projections about the future actions of entities in the environment (Stage 3 SA). Based on the acquired comprehension and projection, decisions are recommended by the AI models to the commanders and then the commanders make the appropriate decisions taking into account the input from the AI and the assessed situation. Finally, the decisions are implemented at the tactical level by the operators. The decisions to be implemented have a vast range including, for example, the positioning of personnel and equipment, firing of the weapons, medical evacuation, and logistics support etc.[19]

Technologies Required for Situation Awareness

Improving sensor data fusion and its consequent SA has been an ongoing process in the field of the armed forces. However, with the speedy development of emerging and disruptive military technologies under the Fourth Industrial Revolution, variety and quality of sensors have

increased manifold, providing real time or near real time SA and with AI, Machine learning, Big Data Analytics and exponentially enhanced computational speed, dynamic decision-making from commander to operator level is increasingly being realised. Various technological advancements are either under consideration or have already been employed by military to improve SA. Some of these are elaborated in the succeeding paragraphs.

Intelligence Collection. Different sources of intelligence that assist in improving SA include human Intelligence (HUMINT), open-source intelligence (OSINT), measurement and signature intelligence (MASINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and geospatial Intelligence (GEOINT). The intelligence acquired from multiple sources is required to filter the discrepancies reported from a particular intelligence source.[20]

Sensors. Technological advancements have led to the development of a multitude of sensors many of which have found applications in surveillance and SA systems. Some of the key sensors are:-

- **Multispectral sensors**. A standard visual sensor collects red, green and blue wavelengths of light. Multispectral sensors collect these visible wavelengths as well as wavelengths that fall outside the visible spectrum, including near-infrared radiation (NIR), short-wave infrared radiation (SWIR) and others. Comprising of three-to-five spectral bands, multispectral sensors fall into two common categories: modified and multiband.[21] Modified sensors are created when a special filter is placed on a standard visual sensor. Multiband sensors are manufactured specifically for multispectral data collection. Each band is collected by a dedicated sensor so there is no need for multiple flights. Multiband sensors mix different band combinations to meet different needs.[22]

- **Radar Sensors.** Radar sensors utilize longer wavelengths at the centimeter to meter scale, which gives it special properties, such as the ability to see through clouds. The spatial resolution of radar data is directly related to the ratio of the sensor wavelength to the length of the sensor's antenna. For a given wavelength, the longer the antenna, the higher the spatial resolution. From a satellite in space operating at a wavelength of about 5 cm (C-band radar), in order to get a spatial resolution of 10 m, one would need a radar antenna about 4,250 m long. An antenna of that size is not practical for a satellite sensor in space.[23]

- **Synthetic Aperture Radar (SAR)** has been developed, wherein a sequence of acquisitions from shorter antenna are combined to simulate a much larger antenna, thus providing higher resolution data.[24] SAR systems provide high-resolution, microwave brightness images of the earth's surface, typically in the 1GHz–10GHz frequency (1cm–60 cm wavelength) range. These images are sensitive to the roughness, geometry and dielectric properties of targets, and thus provide geophysical measurements of the surface.[25]

- Other remote sensing instruments, such as **optical, thermal, and geophysical sensors** measure targets in different regions of the electromagnetic spectrum or through other physical processes (e.g., gravity, magnetism). These sensors are sensitive to different target properties than the SAR, and thus provide information, which is complementary and may be usefully combined with SAR. The data fusion exploits the different information content about a target captured by SAR and other sensors in order to improve the recognition and discrimination of features in the scene. The end-product of fusion through enhancement is typically a colour image in

which the SAR and other data have been combined in to an attractive, interpretable scene.[26]

- **Light Detection and Ranging (LiDAR)** is a popular remote sensing method used for measuring the exact distance of an object on the earth's surface. Even though it was first used in the 1960s when laser scanners were mounted to airplanes, LiDAR didn't get the popularity it deserved until twenty years later. It was only during the 1980s after the introduction of GPS that it became a popular method for calculating accurate geospatial measurements.[27]

Geospatial Technologies encompass Geographic Information System (**GIS**) and Global Positioning System (**GPS**), also known as Geolocation systems:-

- An important aspect of GIS is its ability to assemble the range of geospatial data into a layered set of maps which allow complex themes to be analysed and then communicated to wider audiences. This 'layering' is enabled by the fact that all such data includes information on its precise location on the surface of the Earth, hence the term 'geospatial'.[28]

- GPS when embedded in remotely located sensors provide less than 1 m ranging accuracy in open terrain and less than 2 m ranging accuracy inside buildings.

- The geolocation systems, when utilized for military equipment integrate measurements from complementary sensors to provide a fused solution that is more precise than any individual sensor.[29]

- Through "geolocating" process, locations of places, where videos and photographs are taken, are verified. Geolocation differs from "geotagging". Geotagging is the automated

process of adding geographical identification data to various media such as photographs and videos. Only a fraction of photographs and videos recorded on smart phones, digital cameras, and tablets that are posted online contain an embedded "geotag" of their location. Geolocation techniques, however, allow an investigator to firmly establish the location of recorded images even without an embedded geotag. Using photographs posted on various social media sites, in combination with satellite imagery and "street view" images from services such as Google Earth and Yandex Maps, investigative geolocation techniques pinpoint the coordinates of where photographs were taken.[30]

- Geolocation is thus a powerful and effective tool for tracking individuals and the images they produce. The geolocation methodology was used by combining multiple sources of open domain information to track the movement of soldiers, vehicles, and cross-border shelling from Russia to Ukraine in 2014.

- Geolocation methods enable pinpointing of each piece of equipment to its exact location coordinates using a combination of sources. This includes using satellite and/or ground imagery of the area and matching it with landmarks visible in the media images. For example, in July 2014,a video was uploaded to YouTube showing the movement of a military convoy (carrying 2S19 Msta-S, a self-propelled 152 mm howitzer system) in Rostov-on-Don, Russia, heading west. The coordinates were verified through geolocation, using satellite and ground imagery available through a Russian online map service. Later in September 2014, an Al Jazeera news crew filmed the movement of Msta-S system through Novoazovsk in Ukraine, again heading west.

Comparison of a number of distinctive features in both these videos strongly suggested that the unit was same in both the places and that the unit would have been transferred across the border.[31]

Utilisation of Geospatial and Data Fusion in The Indian Armed Forces

The Governments of India and the United States signed the Basic Exchange and Cooperation Agreement (BECA) on October 27, 2020. The BECA agreement focuses on exchange of Geospatial intelligence (GEOINT) for use by the governments for defence and other purposes. BECA will help India get real-time access to American GEOINT that will improve the accuracy of automated systems and weapons like missiles and armed drones. Through the sharing of information on maps and satellite images, it will help India access topographical and aeronautical data, and advanced products that will aid in navigation and targeting.[32]

In today's Network centric warfare, which is highly dependent on a Multi-platform Multi-sensor data Fusion (MPMSDF) engine, the weapons are launched at a future position of the target. For a dynamic target, errors can lead to serious consequences since the fast-moving hostile fighter jets or incoming missiles may not give a second opportunity to intercept them. Geo-data referencing framework and timing accuracy (via an Atomic clock) are essential for Real-time computation of Air, Surface and Sub-surface warfare functions to achieve a successful missile impact. European nations are employing their Regional Satellite-based Augmentation Systems (SBAS) e.g. EGNOS (European Geo Stationary Navigation Overlay Service) to further improve GPS accuracy and reliability. India too shall have a similar capability when ISRO's PNT (Position, Navigation and Time) services are available using Indian satellite constellations as part of NavIC system.[33]

Geospatial technologies were used fruitfully to establish the location of Russian troops and equipment against Ukraine in 2014. However, that had been categorised under **Digital forensic techniques.**[34] In order to make these technologies as a component of C4ISTAR, these have to be fused with multi-domain, multi-sensor data obtained from varied sources so as to produce near-real-time situation awareness. In July 2020, the U.S. Air Force has reportedly awarded Descartes Labs a contract that will allow them to use the company's geospatial analytics platform for data fusion from multiple sensors including satellite sensors, to provide near-real-time analytics. The contract was awarded by the U.S. Air Force to spark innovation through non-traditional vendors.[35]

Indian Armed Forces should draw a leaf from the U.S. Air Force and engage our emerging start ups along with Indian Space Research Organisation (ISRO) to create / strengthen its C4ISR.

Conclusion

The data collected by a multitude of intelligence, surveillance, and reconnaissance (ISR) sensors enhance the situation awareness of decision makers and help them to better understand their environment and threats. However, this enhancement of situation awareness for end users is impeded by a variety of factors such as: incompatible data formats; bandwidth limitations; sensor persistence (ability of a sensor to sense continuously); sensor revisit time, particularly applicable to satellite or other airborne sensors; and multi-level security. Furthermore, with increasing amount of sensor data, challenge is to identify the most significant pieces of information, fusing that information, and then presenting that information to the end user in a suitable format.

Geospatial technology is now playing a vital role in matters that affect national security, as the professionals working for defence intelligence can now make use of data sharing to their advantage. Geospatial

technology now utilises artificial intelligence (AI) and machine learning (ML) to rectify data processing and analysis issues. These systems allow agencies to gain valuable battle space situational awareness more rapidly and precisely. AI-powered investigation systems also provide forces with a safe and economical way to survey and analyse the hotspots and battlefields in real-time. C4ISTAR based on Geospatial and data fusion technology will act as a Force-Multiplier, providing multitudinous advantage over the enemy. Situation awareness based on Geospatial technology has found great usage in Gray Zone or Hybrid warfare, to detect and identify an adversary, who intends to conceal the identity of its troops and equipment to deny attribution.

***Brigadier (Dr) Rajeev Bhutani (Retd)** is a Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi.

Endnotes

1 Wolfgang Koch, “Target Tracking and Data Fusion for Ground Situational Awareness”, NATO STO LS SET-191, 2013, pp. 5-6.; https://www.semanticscholar.org/paper/Target-Tracking-and-Data- Fusion-for-Ground-Koch/

2. Ibid.

3. Arslan Munir, Alexander Aved and Erik Blasch, “Situational Awareness: Techniques, Challenges, and Prospects”, MDPI, Basel, Switzerland, 29 January 2022, p.56., https://doi.org/10.3390/ai3010005

4. “What are Geospatial Technologies?”, American association for the Advancement of science”, 23 September 2018 https://www.aaas.org/programs/scientific-responsibility-human-rights-law/overview-geospatial-project

5. “What is Geospatial Technology?”, Bronx Community College, http://www.bcc.cuny.edu/academics/geospatial-center-of-the-cuny-crest-institute/what-is-geospatial-technology

6. Jixian Zhang, “Multi-source remote sensing data fusion: status and trends”, International Journal of Image and Data Fusion, Vol. 1, No. 1, March 2010, p.5., https://www.tandfonline.com/doi/pdf/10.1080/19479830903561035

7. “Spatial Data Fusion: Transcending spatial data to the next level”, Ellipsis Drive, https://ellipsis-drive.com/blog/what-is-spatial-data-fusion/

8. Jixian Zhang, op.cit.

9. Mica R. Endsley, Ph.D., “Designing for Situation Awareness in Complex System”, January 2001, p. 4 https://www.researchgate.net/profile/Mica-Endsley/publication/238653506_Designing_for_situation_awareness_in_complex_system/

10. Arslan Munir, Alexander Aved and Erik Blasch, op.cit., p.55.

11. Rolta, “Command & Control: Providing true situational awareness with actionable intelligence for informed decision making and response to emergencies”, http://www.rolta.com/products/rolta-command-control/
12. Arslan Munir, Alexander Aved and Erik Blasch, op.cit., p.56.
13. N. A. Stanton, P. R. G. Chambers & J. Piggott, “Situational Awareness and Safety”, Safety Science 39 189-204, 2001. p.4. https://bura.brunel.ac.uk/bitstream/2438/1804/1/Situation_awareness_and_safety_Stanton_et_al.pdf
14. Arslan Munir, Alexander Aved and Erik Blasch, op.cit., p.57.
15. Ibid.
16. Mica R. Endsley, Ph.D., op.cit., p.4.
17. Arslan Munir, Alexander Aved and Erik Blasch, op.cit., p.58.
18. Ibid.
19. Ibid.
20. Ibid.p.65.
21. “Capturing Multispectral Data using Drones”, https://www.precisionhawk.com/agriculture/multispectral
22 “Multispectral Sensors”, https://www.precisionhawk.com/sensors/advanced-sensors-and-data-collection/multispectral
23 “What is Synthetic Aperture Radar”, Earth Data, https://www.earthdata.nasa.gov/learn/backgrounders/what-is-sar
24 Ibid.
25 Michael Manore and Marc D’lorio, and Jeff Harris, “SAR Data Fusion”, Proceedings of the First Latino-American Seminar on Radar Remote Sensing – Image Processing Techniques, Buenos Aires, Argentina, 2-4 December 1996 (ESA SP-407, March 1997), p-91.
26 Ibid.
27 Bhupendra Sharma, “What is LiDAR technology and how does it work?”, Geospatial World, 02 October 2021, https://www.geospatialworld.net/blogs/what-is-lidar-technology-and-how-does-it-work/
28 “What are Geospatial Technologies?”, American association for the Advancement of science”, op.cit.
29 Arslan Munir, Alexander Aved and Erik Blasch, op.cit., p.65.
30 Maksymilian Czuperski, John Herbst, Eliot Higgins, Alina Polyakova, and Damon Wilson, “Hiding in Plain Sight: Putin’s War in Ukraine”, Atlantic Council, May 2015, p.8., https://www.atlanticcouncil.org/wp- content/uploads/2019/08/HPS_English.pdf
31 Ibid.
32 Shubhajit Roy, “Explained: BECA, and the importance of 3 foundational pacts of India-US defence cooperation”, Indian Express, 03 November 2020, https://indianexpress.com/article/explained/beca-india-us-trade-agreements-rajnath-singh-mike- pompeo-6906637/
33 Milind Kulshreshtha, “US-India BECA agreement for geo-spatial co-operation”, Financial Express, 26 October 2020, https://www.financialexpress.com/defence/us-india-beca-agreement- for-geo-spatial-co-operation/2114139/
34 Maksymilian Czuperski, John Herbst, Eliot Higgins, Alina Polyakova, and Damon Wilson, op.cit.
35 Nathan Strout, “Descartes Labs to provide data fusion platform to the Air Force”, Defense News, 10 July 2020, https://www.defensenews.com/intel-geoint/2020/07/09/descartes-labs-to-provide-data-fusion-platform-to-the-air-force/

59-77

LEVERAGING TECHNOLOGICAL ADVANCES IN C4ISR TO ENHANCE SITUATIONAL AWARENESS AND DECISION MAKING

Gp Capt Amitabh Mathur (Retd), Mr Sandeep Kumar Srivastava, Mr I Prabu*

Abstract

C4ISR refers to technology that offer actionable intelligence for defence and strategic decision-makers to carry out command-and-control directives. Recent advancements in systems, techniques, and technologies have enabled enhanced Situational Awareness (SA) as well as in-depth understanding of an adversary's capabilities. Such enhanced SA will help to minimise the time between the initial perception of a threat and the subsequent decisions generated to mitigate the threat, thereby enhancing C4ISR capabilities. This paper provides a review of current and upcoming technologies that can be used to improve decision-making and SA.

Introduction

The 'nervous system' of the military, a collection of sub-systems used to make the best use of real-time Situational Awareness (SA), is referred to as C4ISR - command, control, communications, computers, intelligence, surveillance, and reconnaissance[1]. C4ISR is the backbone of any defence operation, ensuring battlefield transparency. It gathers and organises data from various sources, analyses them, and then disseminates it to all agencies concerned for coordinated and prompt action.

The value of C4ISR is drastically shifting from a static decision-making process, where commanders used to make decisions based on pre-determined criteria, to a dynamic decision-making process, where the flexibility is built into the system and enables commanders of various commands to interact more effectively in near-real-time and, if necessary, make mid-course corrections.

The quality of data has grown tremendously as a result of advances in electronics, IT, communication, compute power, etc., and this trend will continue. Due to these advancements, massive amounts of data are produced, which may place pressure on analytics to correlate data from many sources, evaluate them, and communicate useful discoveries in almost real-time.

The information used in C4ISR will come from a variety of sources and data types, including satellite and aerial images, pictures, text, audio, and video, sensor data, etc. Aspects to be considered in the implementation of C4ISR are:-

- Common standards and protocols must exist amongst all participating organisations
- Common data formats and data dictionary for seamless exchange of information
- Common GIS with geo-referenced data
- Common co-ordinate projection system
- Standard policies and procedures
- Joint encryption system

This article discusses the design of current and emerging technologies to keep C4ISR relevant and useful for the country.

Architecture for C4ISR

C4ISR receives data from a variety of sources, including services and intelligence organisations. The fact that all of these stakeholders might not want to disclose their internal architecture, including data and apps, is an important consideration in this case. As a result, the joint network centric architecture should be put in place that allows all agencies to share the identified data, when necessary or requested, while keeping other data private.

Each agency has its own secure network, like an 'island'. The network architecture in a C4ISR implementation must be designed to include various 'network islands' with secure points of integration. Autonomy within a 'network island' and secure interoperability across several 'network islands' are key principles to be achieved. Every 'network island' has an Information Exchange Gateway (IEG) that is connected through a data diode. This IEG will only contain the data that has been identified, which will then be shared with the Theatre Shared Data centre (TSD) via a different data diode. This TSD will then transfer data to the Central Shared Data centre (CSD). The IEG of an organisation / agency will not simultaneously connect a 'network island' and a TSD, protecting the private data stored by the 'network islands.'

C4ISR can be implemented in either a centralised or federated architecture. Figure 1 depicts a centralised architecture, in which all the TSD data are centrally stored, analysed, and published in the Client / Server (C/S) model.

In the centralised architecture, all entities will be bereft of ISR support if network communication to the CSD fails. The organisations / agencies shall continue to function in separate vertical silos, with integration between them only conceivable at the CSD level.

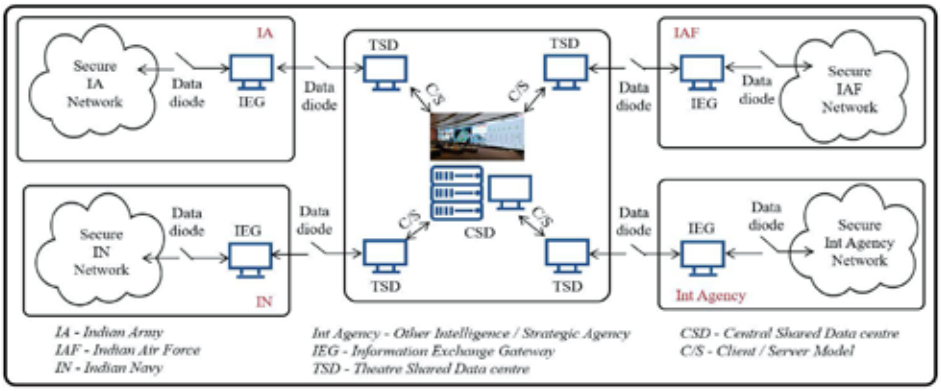


Fig. 1: Centralised Architecture for C4ISR

Figure 2 depicts a federated architecture, in which the TSDs of respective 'network islands' are connected in a Peer-to-Peer model. The IEG of any organisation or agency will gather data from other organisations via the Peer-to-Peer connected TSD. IEG synchronises data with its secure 'network island' whenever the connection to the data diode is established. Redundancy and survivability are better in a federated architecture, due to distribution of resources.

Furthermore, C4ISR architecture will cater for Information Push Model on 'need to know' basis for executors, and Information Pull Model on 'know all basis' for commanders at the decision-making level.

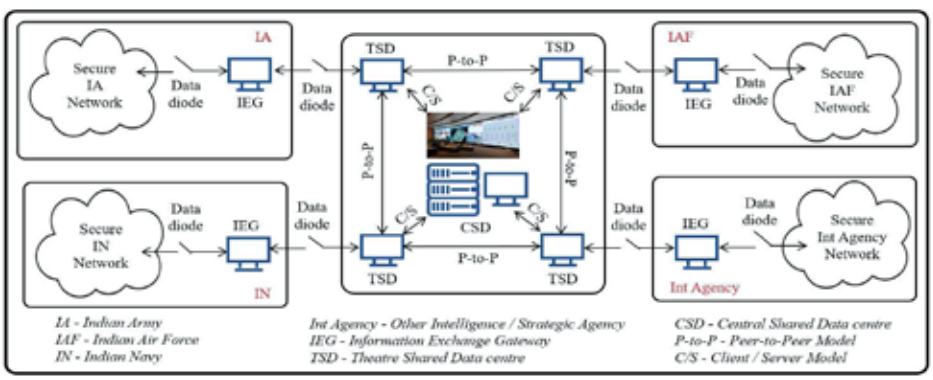


Fig. 2: Federated Architecture for C4ISR

The architecture's subsystems should have proper Sustenance Model, taking into account the centrally manageable Operating System, Compute requirements, scalable Storage, reliable Network, and Cyber Security.

Applications

Applications form the core of SA. Various technological innovations in the past decade have led to enhancements in SA capability. Whether at the services or agencies level or at the Central Command-and-Control Centre, applications are deployed to fulfil the requirements, augment the performance and help in timely and appropriate decision-making capability. Few technologies to improve SA are detailed below:-

- **Data Collection, Collation and Cataloguing.** The development of a significant amount of data at C4ISR, in Network Centric Warfare, is occurring at an accelerated rate, increasing the rate of data flow. This is due to advancements in technology, the deployment of more sensors, the conversion to digital data, among other factors. High-resolution, high-frequency data from satellite and aerial platforms, IoT sensors, surveillance assets, and other sources provide a vast volume of data in the form of images, videos, audio, radio signals, and other types of data. This large volume of data not only presents a challenge in terms of efficient processing, but it also needs high-performance computing systems to provide near-real-time retrieval and analysis of essential data for suitable and prompt decision making.

- Different sources of data collection or intelligence gathering which will help to improve SA are:-

- Human Intelligence (HUMINT)

- Human Intelligence (HUMINT)

- Open-Source Intelligence (OSINT)
- Signals Intelligence (SIGINT)
- Image Intelligence (IMINT)
- Geospatial Intelligence (GEOINT)

Data is available in various categories and formats. Some of the data types for improving SA are:-

- Geospatial data, like image, which are available as satellite images (EO, SAR, IR, Hyper-spectral, etc.), aerial images (nadir, oblique), Vector data (Simple features, Point Cloud, 3D data models, time-series grided data, Data Cubes, etc.), Digital Elevation Models (DEM), Digital Terrain Models (DTM), portrait pictures, landscape images, etc.
- Textual data, like simple text, structured text data, structured database, unstructured text data, Graph database, etc.
- Audio data from audio recordings, phone / mobile call records, electro-acoustic sensors, etc.
- Video data from video cameras, web cameras, surveillance sensors, etc.

Data catalogues, like Spatio-temporal Asset Catalog (STAC), provide a promising solution for semantically classifying, indexing, and organizing data sources across different environments and enriching raw data with metadata[2]. Catalogues of data that include data descriptions may be made available as network services. Implementation of RESTful API discovers and uses data in applications to improve SA.

- **Geo-Spatial Applications.** Geospatial technology is the backbone of C4ISR applications. It offers geospatial image and map analysis capabilities. It also offers users the ability

to understand the landscape, the location of the event, the deployment of the forces and their range, accessibility, changes in time and place, etc.

- **Geospatial Data Publishing.** Geospatial data can be published by following OGC standards (Fig. 3). Geospatial applications can consume the published data in standalone or network mode.
- **Geospatial Image Data Analyses.** Finding new targets, spotting changes, conducting surveillance, planning

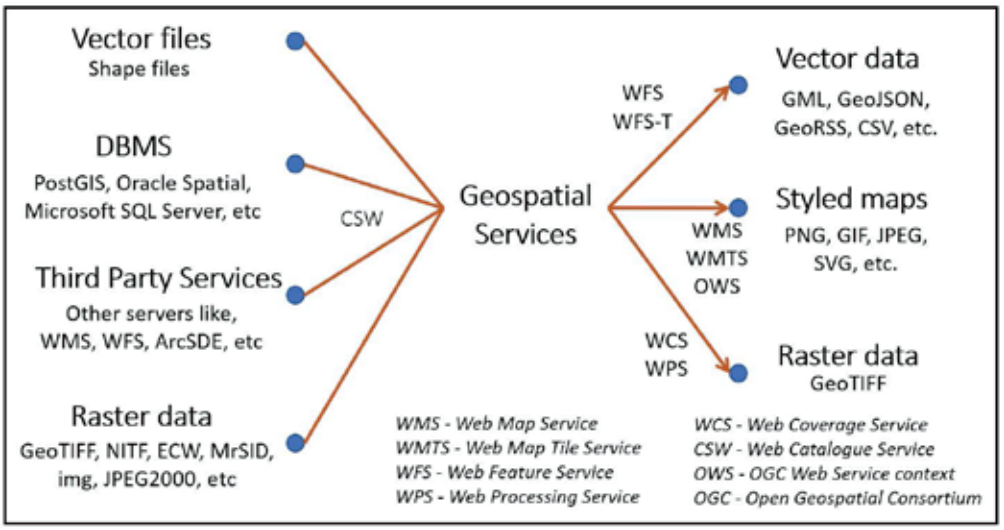


Fig. 3: Geospatial Services

missions, evaluating combat outcomes for Battle Damage Assessment (BDA), Order of Battle (OOB) analysis, etc., are the main goals of analysing geospatial image data from satellites and aerial platforms. They aid in estimating the adversary's military might, locating and tracking the adversary's forces, watching the positioning and disposition of the adversary's military units, keeping an eye on the enemy's primary supply routes, activity

at their weapon storage facilities, course-of-action evaluations, etc.

Mastering the art and science of locating underground silos / bunkers / hidden facilities like ammo dump, will provide critical information for strategic and tactical planning. Geospatial image analyses will play a pivotal role in their identification.

Image interpretation tasks include – feature detection, localization, recognition, identification, comparison, interpretation, understanding, and prediction.

- **3D Terrain Visualization.** 3D landscape visualisation allows Commanders to better appreciate real-world scenarios, while sitting far away from the action. Employing modern 3D projectors / AR-VR / Holographic projections, instead of sand models, enhances their ability to make well-informed decisions.

  Terrain analysis includes numerous surface analysis capabilities, such as locating the highest and lowest points, assessing inter-visibility, determining line of sight, generating view sheds, path profile construction, elevation profile viewing, shaded relief creation, steepest path computation, creating color-coded images for elevation / slope / aspect, displaying slope contours and arrows, cut and fill volume analysis, planning tactical deployment, and 3D fly-through visualisation.

- **Change Detection.** Multi-temporal satellite and aerial photos are examined to detect changes in strategic features. Specific objects identified in a given reference image are compared with features, discovered in the target image, to detect the appearance, disappearance,

or change in placement of objects. Change detection offers useful insight into the behaviour and intentions of adversaries.

The process of automating change detection is currently in development stage. Automation will make it easier to quickly analyse numerous images.

- **Artificial Intelligence Applications.** Robotics and Artificial Intelligence (AI) is the combination of technology and cognitive intelligence for simulation, processing of information, and knowledge to build capability in a machine to imitate human behaviour[3]. Unmanned systems are expected to dominate future wars, and artificial intelligence will be a key factor. On July 11, 2022, the Defence Minister of India launched 75 newly-developed AI products/technologies, at the 'AI in Defence' (AIDef) Symposium, in New Delhi. To modernise defence services and strategic agencies, efforts are currently under way to fully utilise AI's potential. In this perspective, various AI-based applications are explored below:-
  - **NLP Search, Language Support and Sentiment Analysis.** Natural Language Processing (NLP) use Deep Learning (DL) to comprehend the meaning and relationships between words. Intelligence experts employ HUMINT, OSINT, and other types of intelligence data in NLP to derive relevant topic discovery, sequence mapping, and generative summarisation. NLP will provide SA in the context of C4ISR and will improve decision-making.
  - NLP with geospatial technologies may assist agencies comprehend and appreciate the coordination and correlation of events in time and space.

- The technical study and examination of a language form, its meaning, and its environment is known as linguistics. AI plays a critical role in interpreting linguistics in the context of the computer, which will aid in the development of intelligence. Language AI models are available for a variety of tasks such as translation, transliteration, speech to text, text to speech, image to text, and so on.

- Information that circulates through print, electronic, and social media is very valuable to intelligence agencies. Analysis of such data may provide intelligence agencies with important insight into the undercurrents and sentiments of certain groups and/or the general public. Organizations may use NLP to assess public mood, monitor social media, news, and so on, and to categorise online interactions based on emotions such as sadness, grief, joy, rage, and so on. NLP can be used to spot risks, keep an eye on behaviour, and prevent a crisis.

- **O**bjec**t Identification and Classification in Images.** The type of object recognised, its class, and its relative change over time, in a geospatial image, give critical information for C4ISR Commanders, in planning their strategy. AI is a tried-and-tested technique to solve a problem. Of course, the scale of the images and/or photographs have a strong association with the classification of an object. The object should be clearly visible in the image or photograph in order to be classified. Convolutional Neural Networks (CNN) are one of the most used techniques to analyse geographical images. The majority of modern AI detection systems have been trained to recognise pre-defined objects. The future belongs to pre-trained models that will improve SA by

automatically classifying and identifying defence objects and assisting with decision-making.

- **Facial Recognition.** Facial Recognition is a biometric solution that was specifically created and built to recognise the human face, without any physical contact. It can help to improve the security of any organisation or vital facility. The primary goals of facial recognition are to recognise, categorise, confirm, and, if necessary, neutralise any identified threats.

- **Automatic Event Recognition in Video Streams.** Video streams from UAVs, IoT devices, and CCTV cameras are critical sources for surveillance and SA. Automatic video data analysis from diverse sources can aid in the timely analysis of large amounts of data with higher output quality.

  Hidden Markov Models (HMMs) and CNNs require volumes of training data for configuring the network to recognize events. On the contrary, Bayesian networks can be utilized for event recognition when training video data is scarce[4].

- **Super Resolution.** In defence applications, one of the major challenges is to extract information from low resolution images. Super-Resolution can solve this problem. Super-Resolution (SR) is the process of deriving image of higher resolution (HR) by applying an algorithm to low-resolution (LR) images[5].

  In general SR needs multiple images of different resolutions to generate HR images. In defence applications, many times it becomes difficult to get multiple images. Single Image Super-Resolution (SISR)

has fundamental low-level vision problems. The SISR aims to recover the High-Resolution images from a single Low-Resolution image[6].

- Employing Super Resolution on satellite images will enhance the analysis capabilities of C4ISR systems for identification, classification, and change detection of defence targets.

- Advance Applications. Modernization of defence forces and intelligence agencies is headed toward automation, with robots equipped with powerful algorithms analysing available data, applying AI techniques, and making decisions:-

- **Information Fusion.** Surveillance applications use a plethora of sensors, such as motion detectors, proximity sensors, biometric sensors, and a range of cameras, such as colour cameras, night vision imaging cameras, thermal imaging cameras, and so on, to monitor defence targets from various angles and resolutions. Information fusion contributes significantly to SA by helping to extract insightful knowledge from observed data. SA combines low-level information fusion (tracking and identification), high-level information fusion (threat- and scenario-based assessment), and user refinement (physical, cognitive, and information tasks). Information fusion minimizes redundancy between the data captured by different sensors, such as the same or similar views captured by various cameras. Furthermore, information fusion also assists in performing hand off between cameras when an object being tracked by one of the cameras, moves out of its field-of-view and enters into the field-of-view of another camera. In the fog / edge computing paradigm,

information fusion at sensor / IoT nodes reduces the data which are transmitted to the servers[7].

- **Automatic Image Registration / Ortho rectification.** Information extraction with specific geographic location begins with image registration of multi-temporal and/or multi-sensor images. However, the procedure is time and labour-intensive. Automation of the procedures for the near-real-time extraction of meaningful information from satellite and other aerial images is required due to the increasing volume of data coming in.
- Image registration and orthorectification are utilised in defence and security applications such as target detection, recognition, and tracking, vehicle navigation, and surveillance, among other things.
- **IoT and Sensors**
- With the development of new technology, new sensors are developed and used for defence. Soldier health monitoring sensors, autonomous vehicle sensors, gunshot acoustic sensors, and other technologies are being developed to modernise defence systems. They deliver a range of data in various formats to the command-and-control centre, for quick analysis and decision-making.
- **Drone / UAV Data Processing.** Unmanned Aerial Vehicles (UAVs) / drones can greatly assist in enhancing SA because they are capable of gathering intelligence in situations that are regarded dull, unclean, or dangerous. Next-generation UAVs will process the gathered data, perform information fusion, and carry out high-level analytics on board as a result of technological developments. Context-aware UAVs with cameras are

able to produce a high-level description of the scenario seen in the video and pinpoint potentially dangerous circumstances.

The application of drones in novel ways has gained momentum during grey-zone warfare in peacetime. Miniaturization of electronics, new generation navigational tools, and fast computers have resulted in the development of smart weapons, superior sensors with long stand-off ranges, and precise terminal guidance. Loitering munitions, originally developed as anti-radiation drones, have proven to be more dangerous than armed drones.

- **Cyber Warfare.** Cyber warfare refers to the actions of a nation or state or international organisation to attack and attempt to harm another nation's computers or information networks using, computer viruses or denial-of-service assaults. Cyber warfare can take many different forms, including espionage, sabotage, denial-of-service attacks, attacks on the electrical grid, propaganda, economic disruption, and surprise cyber attacks.

  Threat intelligence on the most recent cyber threats, cyber attacks, and zero-day occurrences must be obtained and tracked because they are essential pieces of knowledge for cyber warfare.

  The components of cyber warfare include connecting to the adversaries' network and preventing access to one's own network.

- **Research Areas.** The advancement of technology is a dynamic phenomenon. To keep the system updated, time, money, and resources should be put in researching

emerging / futuristic technology. To gain an advantage over our adversaries, IT development should evolve at a rate that keeps up with global advancement. Below are a few emerging technologies, that are important to defence:-

- **ISAR.** Inverse Synthetic-Aperture Radar (ISAR) is a microwave data processing technique that uses Radar imaging to generate a two-dimensional high-resolution image of a target. It is analogous to conventional SAR, except that ISAR technology uses the movement of the target rather than the emitter to create the synthetic aperture. ISAR radars have a significant role aboard maritime patrol aircraft, which provides them with radar images, for target recognition purposes, like ships and other objects. In situations where other radars display only a single unidentifiable bright moving pixel, the ISAR image is often adequate to discriminate between various missiles, military aircraft, and civilian aircraft[8].

- **Predictive Modelling.** Predictive analytics is a form of advanced analytics that uses current and historical data to forecast activity, behaviour, and trends. It applies statistical analysis techniques, data queries, and ML algorithms to data sets for creating predictive models. Predictive Modelling looks for patterns in data and projects them forward to help the defence sector mitigate risks and capitalize on opportunities[9].

  In the dynamic battle scenario tagging and tracking of defence units like, artillery and armoured columns, in images can enable intelligence units with valuable inputs regarding adversaries planning and motives.

- **5G Network.** 5G network provides ultra-low latency,

which means faster response times when moving data like video and AR/VR for immersive experiences. Its high reliability makes it ideal for supporting mission-critical applications and services. Its massive connectivity capabilities enable faster aggregation of network-connected endpoints, sensors, devices, and data to power IoT connectivity[10].

- **Robotics.** Robotics is a vital tool for executing risky tasks in a defence context, as well as for training, simulating, modelling, and modelling. Robots are being redefined as physically embodied AI entities as a result of continuing technological advancements.

  Robots can be equipped with technologies such as RADAR, electro-optical/infrared, sonar, LiDAR, and others to gather crucial data. Despite being outfitted with sensors and radios, the robots are supposed to be resistant to electronic warfare and cyber-attacks.

- **Quantum Computing.** The field of quantum technology is new and has the potential to be disruptive. The use of quantum technology in the defence, opens up new possibilities while enhancing efficiency and boosting precision, resulting in 'quantum warfare'.

  The 'must-have' technology is the implementation of post-quantum cryptography. The possibility that foreign intelligence is gathering encrypted data with the anticipation of future decryption using the capability of quantum computers is real, high, and present. Few quantum-resilient algorithms can provide not only a new mathematical method challenging enough even

for quantum computers, but also a new paradigm for working with encrypted data.

Interoperability, Standardization and Backward Compatibility

The perspectives of interoperability between two or more system components include information exchange, information understanding, and collaborative coordination between system elements. System interoperability factors such as architectural rationality, security of information exchange environment, operation efficiency, and management maintenance are a few viewpoints to be considered[11].

Integrating diverse platforms from various defence equipment manufacturers employed by each defence / strategic agency is a significant interoperability problem in C4ISR.

Interoperability can be seen from different levels, such as device interoperability, networking interoperability, syntactic interoperability, semantic interoperability, and platform interoperability. These levels, combined with interoperability approaches, openness, connectivity, application protocols, and security / privacy metrics, are required to handle C4ISR Interoperability issues.

Following defence / industry standards in every component is critical to attaining full interoperability. As technology develops, it's possible that outdated hardware and software won't function with new data formats and interfaces. When the hardware, software, or application is upgraded, the existing data should not be lost and should be ready for reuse. Backward compatibility is possible by adhering to standards like ISO, OGC, etc.

Collaboration

It is recommended that agencies collaborate with professional institutes,

for research and development of quality applications. Long-term partnerships with academic institutions will assure future technology research, whilst partnerships with government laboratories and businesses will boost C4ISR by providing cutting-edge applications to run the show.

Conclusion

During a conflict, forces' knowledge of the enemy and the regions where it operates typically decides whether they succeed or fail. In the 1970s, Soviet military strategists invented the phrase 'reconnaissance-strike complex' to explain a networked system that incorporated the modern concept of generating 'kill chains' on the fly by joining an array of sensors to many shooters. Most of the computing power needed by these sensors and networks is already accessible today. Furthermore, additional information may be obtained via the cloud and fed into AI systems, resulting in newly accessible and affordable ways of seeing and techniques for bringing together and analysing the data collected and presenting the information as and when needed. AI systems also address stealth, electronic warfare, cyber attacks, and other forms of deceit that hiders can use to remain undiscovered. As a result, the reconnaissance-strike complex has grown in sophistication. Modern day architects are merging technologies to develop a system that can quickly eliminate a large number of potential targets while passing information about them to the essential locations.

***Gp Capt Amitabh Mathur (Retd)** expertise in IAF is on maintenance of Surface to Air Guided weapons, Electronic Warfare and Specialist Air Weapons.

Mr. SK Srivastava has extensively worked in application of geospatial technologies for more than three decades while serving as Senior Director & HoD at C-DAC, Pune. Presently, he is working as Consultant – Strategic Projects at C-DAC, Pune.

Mr. I Prabu is currently working as the Joint Director in Geoinformatics domain at C-DAC, Pune. He has led teams for development of applications in the defence and strategic sector.

Endnotes

1. C4ISR: The Military's Nervous System, 7 January 2020, https://www.defenseone.com/insights/cards/c4isr- military-nervous-system/?oref=d1- cards-prev-nav
2. Ehrlinger, Lisa & Schrott, Johannes & Melichar, Martin & Kirchmayr, Nicolas & Wöß, Wolfram. (2021). Data Catalogs: A Systematic Literature Review and Guidelines to Implementation. 10.1007/978-3-030-87101-7_15.
3. Kavita Nagpal, 2022, "Artificial Intelligence in Defence Sector"; https://defproac.com/?p=7231 accessed 22 August 2022.
4. Munir, A.; Aved, A.; Blasch, E. Situational Awareness: Techniques, Challenges, and Prospects. AI, 2022, 3, 55–77. https://doi.org/10.3390/ai3010005
5. Chao Dong, Chen Change Loy, Xiaoou Tang.; Accelerating the Super-Resolution Convolutional Neural Network.; Computer Vision – ECCV 2016, 2016, Volume 9906, ISBN: 978-3-319-46474-9.
6. Vijaysinh Lendave.; Guide to Image Super-Resolution By ESRGAN.; 10 July 2021; https://analyticsindiamag.com/guide-to-image-super-resolution-by-esrgan/
7. Wikipedia, "Inverse synthetic-aperture radar", last modified 23 June 2022 at 18:59, https://en.wikipedia.org/wiki/Inverse_synthetic-aperture_radar
8. Linda Tucci., What is predictive analytics? An enterprise guide, December 2021; Techtarget, https://www.techtarget.com/searchbusinessanalytics/definition/predictive-analytics, accessed 14 August 2022.
9. Emma Helfrich, 5G and the military: A new era of connectivity, Military Embedded Systems, 19 October 2021, https://militaryembedded.com/comms/communications/5g-and-the-military-a-new-era-of- connectivity, accessed 16 August, 2022.
10. M. F. Muller, F. Esmanioto, N. Huber, E. R. Loures, and O. Canciglieri, 'A systematic literature review of interoperability in the green Building Information Modeling lifecycle,' J. Clean. Prod., 2019, doi: 10.1016/j.jclepro.2019.03.114
11. M. Noura, M. Atiquzzaman, and M. Gaedke, 'Interoperability in Internet of Things: Taxonomies and Open Challenges,' Mob. Networks Appl., vol. 24, no. 3, pp. 796–809, 2019, doi: 10.1007/s11036-018-1089-9.

ADVANCING C4ISR CAPABILITY: LEVERAGING EMERGING TECHNOLOGIES AND COMMERCIAL ADVANCES

Gp Capt Puneet Bhalla*

Modern military operations are expected to involve increasingly diverse and intricate operational scenarios requiring missions to be conducted across multiple domains and effects. The expanded battle spaces have increased the breadth and depth of information desired in real time. Commanders have to plan for a wider range of missions, from those involving high tempo of operations that mandate prompt responses, to long drawn face-offs that depend on force capability, deployment and sustenance for deterrence. Complexity has been further added by the introduction of newer domains of space and cyber and of novel technologies and weapon systems. Military strategies as well as compulsions of resource constraints, of both equipment and manpower, are compelling the precise use of combat elements, achieving the desired results while ensuring economy of effort. The increased dynamism of manoeuvre in an expanded battlefield space has reduced the decision-making timelines, with the advantage going to the side that can stay ahead in these processes.

It has been evident for some time now that enhancing operational efficiency requires a shift from the platform-centric approach to one that leverages technology for optimum employment of combat elements. Command and Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems are labelled as the

"nervous system" of the military. They enhance situational awareness (SA) and knowledge of the adversary and environment, provide support in planning, offer decision advantages to the commanders, allow novel concepts of operations and assist in the synchronised management of combat related operations. They are thus force enhancers that depend on technological solutions to provide a competitive edge against the adversary.

C4ISR is an amalgamation of various subsystems, each contributing to the overall efficacy of the system. There is a heavy dependence of these on information and communication technologies (ICT) and an asymmetric advantage would be gained by the side that could better apply developments in these as well as exploit emerging technologies and innovative technological applications towards capability enhancement. Traditionally, militaries have depended on government funded R&D and a lot of new age technologies have emerged from these programs. This has changed in recent years as the necessity of quick, innovative and resilient solutions in an increasingly competitive and contested civil and commercial space is becoming as essential as in the military domain. This has incentivised private investments in technology development, especially those related to ICT.

Artificial Intelligence (AI) is a technological tool that has applications across domains to improve efficiencies, accuracies and help in decision making. Machine Learning (ML) is a subset of AI that allows the system to operate more autonomously, adapting to the dynamic environment and progressively improving their responses. Both are finding important applications in the modern military operational environment, especially among C4ISR systems, that are highly dependent on IT enabled applications and services. The article would cover a few of the envisaged advances in technology and assess the leveraging of developments in the civil domain to achieve information superiority and stay ahead in the decision making and execution cycle.

Intelligence, Surveillance and Reconnaissance (ISR)

The ISR process involves information acquisition through multiple sensors, having the necessary communication capability to ensure timely transmission of information, adequate storage and processing capability for the huge amount of assorted data, and the ability to provide actionable intelligence to decision makers, where required, in a format that is easily comprehensible.

Sensors. The wide expanse of operational areas and the accelerated rate of operations dictates increasing the numbers and diversity of distributed sensors across multiple domains, including those of space and cyber, to address the spatial, spectral and temporal gaps. Space offers resilient and secure multi-spectral capability, mainly from Low Earth Orbit. Digitisation and miniaturisation have enabled the production of smaller satellites with comparable capabilities. Private entities are now fielding imaging constellations with advanced capabilities that reduce the time between scans through numbers and provide multi-spectral imagery at affordable costs. Pixxel, an Indian start-up, launched the first of its satellites, Shakuntala, claimed to host the 'world's highest resolution hyper spectral commercial cameras that has ever been flown to space', on SpaceX's Falcon-9 rocket. There is also a proliferation of Unmanned Aerial Systems (UAS) that could be equipped with varied sensor payloads. Capabilities of both platforms and payloads are being developed by private players for a variety of civilian roles that have applicability to military ISR too. An agile and resilient sensor architecture that connects sensors and weapons across mission areas would greatly enhance the efficacy of operations.

The complex battlefield necessitates real time information across vast areas and domains, even as the sensors of requisite capabilities remain scarce. AI could be gainfully applied to automatically prioritise, cue and optimise ISR platform and sensor use to maximize the probability of target detection and identification. An appropriately designed closed

loop system would enable dynamic resource allotment to cater to the evolving operations and the command intent.

AI capability onboard distributed platforms would help optimise the use of interlinked machines by improving the decision-making capabilities and contextual awareness of robots towards working cooperatively towards common mission achievement with minimal human interaction. Swarm UAV demonstrations, involving autonomous formations of scalable machine-to-machine teams, are already demonstrating their prowess and could be programmed for various C4ISR related functions. U.S. DoD's Defense Advanced Research Projects Agency's (DARPA) Context Reasoning for Autonomous Teaming (CREATE) program seeks to develop the theoretical foundations of autonomous AI teaming to enable a system of heterogeneous, contextually-aware agents to act in a decentralized manner and satisfy multiple, simultaneous and unplanned missions' goals.[1] This technology would greatly enhance the functionality and capability of unmanned swarms in support of ISR missions.

Geospatial Systems. Military operations are planned and executed in a geographical space and would benefit from georeferenced data. Besides reducing the processing requirements, it would provide context to the information. Space enabled Position, Navigation and Timing services contribute immensely to these efforts. Geospatial tools also enable digital terrain modelling and projection of geographical and military data onto digital maps for better appreciation of threats, patterns and trends. Georeferenced projections allow more synergised planning and execution of operations, optimising support missions and reducing chances of fratricide. Additional applications and map products could be developed to provide enhanced capabilities for decision-making.

Communication and Network Technologies. Information assurance would require communication networks' infrastructure that is robust, agile, secure, resilient and adaptable and has sufficient capacity to handle the large volume of data being generated by an increasing

array of sensors. The highly dynamic battlefield environment consists of distributed and displaced mobile command posts and forces that need to be orchestrated in real time by timely conveying of command decisions. Redundancy can be achieved through a network of dispersed heterogeneous groups of communication equipment with expansive coverage. Last mile connectivity would require wireless connectivity.

Space Enabled Communications. Space is being revolutionised with the addition of LEO-based distributed communication capability that reduces latency, enhances coverage and greatly adds on the transmission capacities. This capability is supplementing the already increasing communication capabilities through deployment of High Throughput Satellites in the conventional GEO and Optical Communication. LEO-based communication constellations are being developed by private entrepreneurs like SpaceX and OneWeb and provide options in terms of technology and capabilities that the military systems could exploit. A pertinent example is of the ongoing Russian-Ukrainian War, where access to open internet has been resorted to for transmission of information and C2 by both sides to overcome electronic disruption. A significant event of the conflict was the continued provision of internet to Ukrainian soldiers through the private Starlink LEO-based satellite internet network, when Russian EW and cyber efforts were able to achieve disruption of SATCOM services from the American Viasat network. Interestingly, the private company was able to counter similar Russian disruption against its own systems, ensuring continued last mile connectivity through hundreds of terminals provided to the Ukrainian forces.

5G Networks. These are already being progressed for commercial services that would provide higher data transfer capacity at significantly higher speeds. It has applicability for military networks, especially for last mile connectivity. China has already deployed 5G networks for information flow in border areas of Eastern Ladakh. Indian Armed Forces have also actively followed up on the introduction of 5G for civil networks

by conducting a Joint Services Study that has deliberated upon and recommended a roadmap for the induction of 5G. An MoU has been signed between MCTE and IIT Madras for the setting up of a test bed that would facilitate the validation of military use cases of 5G.[2]

Software Defined Communication. Software defined communication devices that would be capable of hosting multiple waveforms and operating over multiple orbits and frequencies is vital for communicating in a dense electromagnetic environment susceptible to jamming, interference and outages. These would be portable and easy to reconfigure and could even employ AI for more autonomous functioning.[3]

The armed forces are already assessing the network-centric potential of both legacy and developing systems and work is afoot on different sets of multimodal communication networks to enable the coordinated use of forces and collaborative targeting. Communication technologies involving satellite enabled networks, wireless communications, including 5G networks and software defined radios, would have to be leveraged to provide multi-layered architecture for enhanced capacities, lower latencies and redundancy. AI also has applications for Electromagnetic Spectrum Operations (EMSO) – mission specific networking and dynamic bandwidth allocation for use in degraded communications conditions and for enabling proactive and responsive network protection (Electronic Warfare).

While commercial communication systems are not traditionally designed to function in contested environments, collaborative efforts could help exploit advances in civil networks towards upgrading existing military systems or could assist in developing enterprise communication architectures to meet military standards. Commercial private networks could also be exploited for emergent military operations, when organic communication capability has not been deployed or has been degraded. In the U.S., its Army is pursuing an Integrated Tactical Network that incorporates a Secure but Unclassified (SBU) communications

architecture into the network. This allows soldiers to leverage commercial cellular networks—such as 4G, LTE and WiFi, along with other commercial wavelengths—to communicate. This is expected to enable the forces to be more expeditionary and mobile.[4] Its DoD is also focussing on Joint All Domain Command and Control (JADC2) through open architectures and interoperability and these modernisation goals and objectives are being pursued through commercial solutions.[5]

Data Processing. Computers enhance the processing power of information and decision making and consequently of the timeliness and efficacy of Command and Control (C2). The proliferation of ISR sensors is resulting in a deluge of complex data from service specific sensors and from other diverse sources. These could be operating in different spectral bands of the electromagnetic spectrum, imaging from varied positions in terms of heights and angles and have diverse software standards. Leveraging data for information dominance would necessitate integration of the varied data, tested for its accuracy and processed for relevance to provide value addition to the decision making. This is a challenge considering that most of the sensing systems belong to differing legacies and domains and have evolved disparately, leading to incongruent formats. Innovative computing solutions are required to scale up the processing capability to address subsequent enlarged data handling functions.

Cloud Technology. This huge volume of intelligence data would have to be stored for future analysis and reference purposes in a format that could be easily shared, when required. Cloud technology allows the use of shared IT infrastructure and services that go beyond storage to cloud computing – through the flexible, scalable and on-demand IT environment.

Deployable Clouds. While server farms could be distributed for better network management and redundancy, another application offering options for military operations is deployable clouds. This would reduce

the dependency on networks and latency in transmission of data, while enhancing the ability of the field commander to take decisions as part of more evolved decentralised execution.

Edge computing. It is a concept involving distributed, networked autonomous sensors, allowing data to be processed on the spot at the "edge" of the network, i.e., AI enabled processing at the level of sensors, or nearby. This helps in cutting down the processing time, speeding up the sensor to shooter cycle and lowering the exposure to network vulnerabilities and limitations. It also reduces the need for large processing centres that could be vulnerable to physical and virtual attacks.[6] The importance of cloud infrastructure has grown significantly in recent years, further accelerated due to challenges thrown up by the Covid-19 pandemic. Strategic cloud solutions being developed by companies for business applications could be applied to national security efforts. Thales is working on the world's first theatre-level deployable defence cloud capability for NATO's Deployable Communications and Information System (DCIS). This project will utilise private cloud architectural principles and functions like automation and orchestration to significantly reduce the time to configure, deploy and activate services to the soldier. The new project will be based on work previously done with the industry to develop an architecture for a new DCIS.[7]

Manual operations for fusing this data, spread across many different databases and stakeholders, is arduous and time consuming, even with the help of the high computational prowess of contemporary machines. AI and ML algorithms and processes would lead to automated sensor data fusion with ultra-low latency. Human resources are also limited in capacity and skills to analyse the data to accurately produce results of relevance. AI would enable high-speed autonomous scrutinizing of data, with appropriate algorithms turning the information into coherent, actionable intelligence to speed up the decision making. For example, on the basis of algorithms, convolutional neural networks (AI systems designed to process images) are able to pick out objects of interest

automatically. Linking the system to diverse libraries of relevant data would enable next-level intelligence functions such as anomaly detection, automatic feature extraction for target identification and characterisation and automatic characterisation of operational areas.

Rafael Advanced Defence Systems Ltd has demonstrated a new Automatic Target Recognition (ATR) capability for its SPICE-250 air-to-ground, stand-off, autonomous weapon system which can utilise this capability to autonomously detect and recognise its individually assigned target.[8] Project MAVEN is a U.S. DoD's initiative that aims to use AI to decipher aerial surveillance footage to improve targeting for UCAVs.[9] The Indian Army has developed in-house algorithms to analyse in real-time the inputs coming from various sensors in the field. The system is capable of handling heterogeneous inputs from diverse sensors and an AI-based real time monitoring software has considerably reduced the requirement of human involvement. It is collaborating with DRDO and academia for this.[10] Private companies in the digital domain are already acquiring petabytes of data from multiple sources and devices, and sifting through it to provide personalised feed for its billions of users. This ICT capability could be harnessed for military systems.

Decision Making. Enhanced computing would also contribute to timeliness of decision cycles at all levels of command. AI has emerged as an important component of decision-making processes and algorithms could be suitably developed or modified for military applications.

Decision Options. As battlefield complexities continue to rise, AI could be employed to assist the commanders by offering courses of actions and their probable outcomes at exponentially faster speeds. For example, the system could offer target prioritisation options for a particular outcome over a given area. ML could be utilised to improve the computed responses of the C4ISR system over regular gaming of situations.

Predictive Analysis and Inputs. AI and ML could also be programmed to develop capability towards predictive analysis and inputs. This would

greatly enhance the response options and timelines. This has relevance in all physical and virtual domains. For example, systems could be programmed to generate preconfigured responses to electronic warfare (EW) and information warfare (IW) attacks. Predictive threat analysis is already a part of cyber security efforts and could provide the foundations for similar efforts in other domains. An example of this concept is Project Kaiju, a U.S. Air Force Research Lab's effort which is exploring AI/ML-related technologies and resources to advance EW technology against emerging Integrated Air Defence System (IADS) capabilities.[11]

Visualisation

Common Operating Picture (COP). SA would be greatly enhanced through the projection of simple, intuitive, geo-referenced intelligence onto a common display. Task complexities could be reduced towards more efficient planning, decision making and battle management. Joint operations would ordain integrated information display covering multiple domains to consolidate all warfighting information onto a common operating picture (COP) that would also support multi-domain manoeuvres in real-time. Immersive technologies like Augmented Reality/ Virtual Reality, and now the evolving Metaverse being developed for multiple commercial applications, could have applications for enhancing SA and assist in decision making.

Tactical level SA could be enhanced through the provision of relevant information onto wearables or platform mounted screens. It is important to design these for easy assimilation and with minimal task complexity through user-friendly interfaces and optimised interlays for ease of use. Private companies consistently strive to enhance visualisations and interfaces and this experience should be exploited for military systems too. North Atlantic Treaty Organisation (NATO) has contracted with Thales to supply the new increment of the NATO Common Operational Picture (NCOP) programme. This is expected to be achieved through layers of maps and referenced information on battle space objects operating in

all domains.[12] Information sharing and decision making could also be supported through apps for SA and C2. Applications based on social media and chat structures could be incorporated for more interactive processes towards information exchange and decision making.

AI would help ease the process of sharing of information to relevant decision-making nodes through 'push' rather than 'pull' processes, autonomously. The 'pull' principle works on data being queried from the system, whereas the 'push' principle involves predictive provision of appropriate data to the user, based on the mission and operational environments. The tools already exist in the social media platforms, wherein advertisements are forwarded to consumers based on their surfing history, without being queried.

Joint C4ISR

There is a growing emphasis on joint operations and Joint C4ISR would enable flexibility in composition, deployment and employment of force packages to meet their evolving objectives and enable the coordinated application of combat power. The aim for an integrated C4ISR architecture, although desirable for a long time now, has faced its challenges in terms of technology, service specific command and control practices, cognitive variations and budgetary limitations. A U.S. Navy Study had recommended the attributes of composability and adaptability in the service specific capabilities. Composability is a system design principle that deals with the inter-relationships of components, allowing components to be selected and assembled for mission specific combinations of platforms and sensors in each layer. They would depend on a local-area network for tasking and collection and processing of data to create a tactical picture that meets the commander's needs for that mission area.[13] Adaptability is the longer-term goal of using military systems in missions for which they were not originally intended, in response to dynamically changing situations and/or real-time events.[14] Equipment adaptability should also facilitate future upgrades as

advances in C4ISR technology mature and are implemented.

Interoperability

The key to effective joint C4ISR lies in optimising the functionality and interoperability of disparate domain/ service specific components and systems. Contemporary systems and technologies have been procured or developed in isolation, with little consideration to interoperability, even within the services. The same holds true for communication networks that have been developed for specific systems or functions, resulting in silos. They require manual processes and inputs to accomplish mission tasks, entailing time critical delays and affecting accuracy of data. Interoperability among systems would allow more autonomy to be enmeshed into the systems that would provide advantages in terms of data handling and processing.

Developing a Common Operating Environment (COE) would be achieved through integrating hardware and software systems, requiring standardisation of equipment and protocols. Development of futuristic C4ISR systems should be based on Enterprise Integration, which would involve creating an open digital ecosystem that would better enable connecting components and systems through adoption of these measures. Open architecture approaches would enable exploiting modern hardware and software solutions being developed commercially to achieve interoperability among digital devices. The armed forces could use the service-oriented architecture (SOA) approach, which has been developed in the commercial sector for enterprise software systems, to enable interoperability. SOA defines a way to make software components reusable via service interfaces that utilise common communication standards in such a way that they can be rapidly incorporated into new applications. This allows users to combine functionality from existing services without requiring deeper integration of existing systems.[15]

Acquisition process would have to be streamlined to acquire or develop sub-elements of planned C4ISR architecture that follow defined standards for interoperability, even when acquisition follows a multi-track or multi-vendor option. This would dictate smooth funding and streamlining of arduous bureaucratic procedures. Innovation would also be enabled by involving academia and laboratories through incentivised, time-bound funding of next-gen foundational technologies.

Private Participation

The military remains sceptical of the capabilities available in the civil domain and their applicability to its operations. Concerns relate to limited experience in applying commercial approaches to military applications, the ability of commercial products to address the scale of military operations and the adequacy of security protocols among these systems.

A lot of effort in the civil domain is aimed at seeking solutions for information handling and decision making towards maximizing the operational and business effectiveness; these have applicability to military C4ISR systems. Constant endeavour is also being made at enhancing technological prowess and refining protocols and processes, while exploring more emerging technologies and applications to constantly improve upon these capabilities, achieving rationalisation of the effort in terms of time and resources. Advanced technology, hitherto dominated by government institutes and large conglomerates, is seeing an increasing participation by medium enterprises and even small start-ups. The resultant increase in competitiveness is beneficial for technological developments, innovation and a higher diversification in offered products. Diverse strategies of the commercial domain that include partnerships and collaborations and mergers and acquisitions lead to faster technology maturation and operationalisation.

Military professionals would have to collaborate with experts with a

greater understanding of technology to identify ways to bring those technologies and solutions into the operational environment, and for the collaborative development of futuristic systems and architectures. Adaptation of such solutions in the military will come with corresponding savings in terms of time and costs, but would have to emphasise on security of data.

Global Efforts

The U.S. is taking an integrated approach towards utilising AI for military applications. It established a Joint Artificial Intelligence Center (JAIC) in 2018, with a focus on C4ISR systems. The strategy included partnering with leading private sector technology companies, academia and global allies and addressing the Human Resource development issues.[16] It has now been placed, along with the Defense Digital Services (DDS), the Chief Data Officer, and the enterprise platform Advana into one organization, the Chief Digital and Artificial Intelligence Officer (CDAO), which became operational on 01 Jun 2022. The aim is to build a strong foundation for data, analytic, and AI-enabled capabilities to be developed and fielded at scale.[17] China's commitment to enhance the prowess of its C4ISR systems is evident in the reorganisation effort that centralised space, cyber and electronic warfare under the newly established PLA Strategic Support Force and its investments in cyber capabilities and futuristic technologies like AI. In the U.K., Joint Concept Note (JCN) 1/20 has spelt out Multi-Domain Integration (MDI), founded on the Integrated Operating Concept, aiming to integrate operations across the domains and levels of warfare, as also with other national entities and networks. It also provides a vision for the development of an integrated force out to 2030 and beyond.[18] There are similar efforts being pursued across the globe, many of them in collaboration with globally established private defence contractors. Consequently, the C4ISR market is projected to grow from USD 119.9 billion in 2021 to USD 147.1 billion by 2026, at a CAGR of 4.2%.[19]

Conclusion

Across the spectrum of military operations, it is clear that the advantage would lie with the commander who has better situational awareness and swift decision-making tools and capabilities at his disposal and can ensure that his plans are executed expeditiously. C4ISR best defines the interdependency between technology and military operations. Foundational C4ISR architectures have been put in place by most major militaries but the requirement is of constantly improving upon the sophistication of equipment and seamless integration across all warfighting domains and functions. Indigenisation is a necessity for economic as well as security considerations. As India intensifies its efforts at *Atmanirbharta*, IT related development is one of the strengths of its industry that could be judiciously utilised to reduce the reliance on defence imports. The pace of technology upgradation is so rapid that conventional acquisition processes need to be overhauled so that the technology remains relevant. Another challenge is the way this IT based technology would be shared or owned. This would require modification of existing budgetary and acquisition processes to keep up with the rapid pace of technology development and to cater to newer technological domains. For example, AI is a software-as-a-service (SaaS) model, which would require a different approach from the existing buying model.[20]More importantly, it necessitates a change of mindset towards collaborating with the private industry.

***Gp Capt Puneet Bhalla** is a Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi.

Bibliography:

1. Defence One, “C4ISR: The Military’s Nervous System”, [Online: web], Accessed Jul 2022, URL: https://www.defenseone.com/insights/cards/c4isr-military-nervous-system/4/?oref=d1-cards-next-nav

2. AK Sachdev (2022), “C4ISR and Autonomous Capabilities”, [Online: web], Accessed Jul 2022, URL: http://www.indiandefencereview.com/news/c4isr-and-autonomous-capabilities/

3. Airforcemag (2022) “AI for Faster Decision-Making”, [Online: web], Transcript of AFA Warfare Symposium, March 4, 2022, Accessed Jul 2022, URL: https://www.airforcemag.com/watch read-future-isr-will-include-ai-for-faster-decision-making/

Endnotes

1. Aaron Kofford, 2019, “Context Reasoning for Autonomous Teaming (CREATE)”, [Online: web], Accessed 18 Jul 2022, URL: https://www.darpa.mil/program/context-reasoning-for-autonomous-teaming
2. Dinakar Peri, 2022, “Army deploys AI-based solutions to augment real-time surveillance”, The Hindu, 06 August 2022. https://www.thehindu.com/news/national/army-deploys-ai-based-solutions-to- augment-real-time-surveillance/article65737335.ece
3. Lou Dubin, 2022, “Smarter Comms for a Modern Military—facing an adversarial world”, URL: http://www.milsatmagazine.com/story. php?number=1904895511, accessed 12 July 2022
4. Devon L. Suits, 2019, “New tech, accessibility to improve Army tactical networks”, Army News Service, URL: https://www.army.mil/article/223507/new_tech_accessibility_to_improve_army_tactical_networks, accessed 18 Jul 2022
5. National Research Council, 2006, “C4ISR for Future Naval War Strike Groups”, National Academics,URL: https://nap.nationalacademies.org/ catalog/11605/c4isr-for-future-naval-strike-groups, Accessed 10 August 2022
6. John McHale (2022), “Military AI speeds up human decision-making”, URL: https:// militaryembedded.com/ai/machine-learning/military-ai-speeds-up- human-decision-making, accessed 16 July 2022
7. NATO Communications and Information Agency, 2021, “Agency awards Firefly contract for deployable communications and information systems”, URL:https://www.ncia.nato.int/about-us/newsroom/agency-awards-firefly-contract-for- deployable-communications-and-information-systems.html, accessed 30 July 2022
8. Air Force Technologies, 2021, “Spice 250 Precision Guided Munition”, URL: https://www.airforce-technology.com/projects/spice-250-precision-guided- munition/ accessed 30 July 2022
9. Thomas Brewster (2021), “Project Maven: Startups Backed By Google, Peter Thiel, Eric Schmidt And James Murdoch Are Building AI And Facial Recognition Surveillance Tools For The Pentagon”, Forbes, URL: https://www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-startups-backed-by-google-peter-thiel-eric-schmidt-and-james-murdoch-build-ai-and-facial-recognition-surveillance-for-the-defense-d- epartment/?sh=1ee22c196ef2, accessed 30 July 2022
10. Dinakar Peri, 2022, “Army deploys AI-based solutions to augment real-time surveillance”, The Hindu, 06 August 2022. https://www.thehindu.com/news/national/army-deploys-ai-based-solutions-to- augment-real-time-surveillance/article65737335.ece

11. Journal of Electromagnetic Dominance, 2021, “Air Force to Develop AI/ML EW Technologies Under Project Kaiju” URL: https://www.jedonline. com/2021/10/27/air-force-to-develop-ai-ml-ew-technologies-under-project-kaiju/, Accessed 03 August 2022
12. Norbert Neumann, 2022, “Chains of command: Inside Thales’ C4ISR capabilities”, [Online: web], Accessed 15 Jul 2022, URL: https://www.army-technology.com/uncategorized/c4isr-c4i-thales-command-and-control/
13. National Research Council, 2006, “C4ISR for Future Naval War Strike Groups”, National Academics, URL: https://nap.nationalacademies.org/ catalog/11605/c4isr-for-future-naval-strike-groups, accessed 10 August 2022
14. ibid
15. IBM Cloud Education, 2019, “SOA (Service Oriented-Architecture)”, URL: https://www.ibm.com/in-en/cloud/learn/soa, accessed 05 August 2022
16. Chief Digital and Artificial Intelligence Office, 2022, “The JAIC Story: Five Pillars of the DoD AI Strategy”, URL:https://www.ai.mil/about.html, accessed 05 August 2022
17. Chief Digital and Artificial Intelligence Office, 2022, “Chief Digital and Artificial Intelligence Office (CDAO), URL: https://www.ai.mil/cdao.html, accessed 05 Aug 2022
18. Government of United Kingdom, 2020, Multi Domain Integration (JCN 1/20), Ministry of Defence, London
19. Markets and Markets, 2021, “C4ISR Market by Solution, Platform, Application, End User, Installation And Region - Forecast to 2026”, URL: https://www.reportlinker.com/p04397142/C4ISR-Market-by-Platform-Application- Component-and-Region-Forecast-to.html?utm_source=GNW Summary Accessed 01 Aug 2022
20. John McHale, 2022, “Military AI speeds up human decision-making”,URL: https://militaryembedded.com/ai/machine-learning/military-ai-speeds-up- human-decision-making, accessed 16 Jul 2022

SPACE BASED JOINT C5ISR CAPABILITY BUILDING

Lt Gen A B Shivane, PVSM, AVSM, VSM (Retd)*

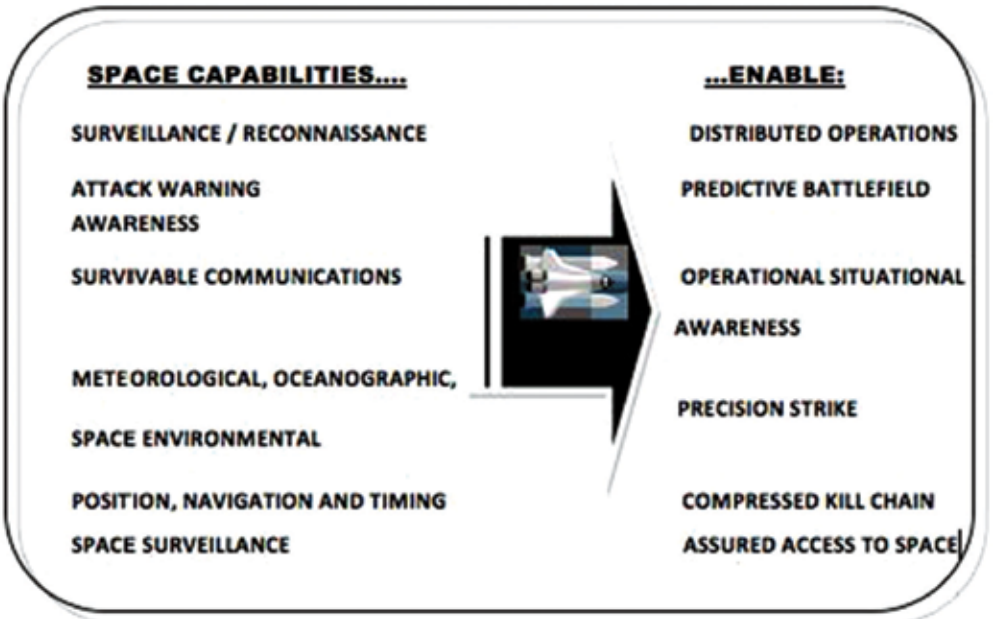
"Future global rivalries would keep nations in an attritional posture in a wide range of fields…i.e. economical, technical knowledge, scientific breakthroughs and energy rivalries in a protracted infinite time scale. The concept of wars would become outdated to be replaced by spontaneous short and decisive engagements. However, netwars may create a new dimension of warfare in the 21st century requiring combined Space, air and specialized ground operations in a protracted time frame."

***Rig Veda 1200* – 900 BC**

Joint Force Capabilities in Future Conflicts

The future wars will be fought in all seven domains - land, air, sea, sub-surface, space, cyber and cognitive domain in a network-enabled environment. The key determinant of success in future conflicts across the entire spectrum will be astute leadership empowered by information superiority, decision dominance and a compressed kill chain under disruptive conditions. This would result in higher favourable exchange ratios enabled by shortened OODA loop. The net desired outcome will be victory at least cost and minimum time by dominating the key factors of time, space, force and information. The joy of its outcome will be to get the right information, at the right time, at the right place to the right person without information overload through an integrated C5ISR(Command, Control, Computers, Communications, Combat Systems, Intelligence, Surveillance and Reconnaissance). Accordingly, the four core decisive joint force capabilities in future battle space will be - Information Dominance (Information), Shared Situational Awareness (Space), Decision Dominance (Time) and Joint Force Synchronisation (Force). In short, we need a knowledge-based; decision-oriented, networked, joint force space enabled C5ISR capability.

The exploitation of space-based capabilities and generation of space assets have transformed contemporary warfare with very significant improvements in situational awareness, distributed operations, predicted battle space awareness, and precision strikes in a network-enabled joint force environment. The resultant kill chain of *"find, fix, track, target, engage and assess,"* has been markedly reduced. Space systems have thus graduated from their role of being *"force enhancers"* to assets that are *"force enablers"*.



Strategic Military Surprise - An Indian Faultline

Military strategic surprise has repeatedly haunted the Indian security apparatus since independence due to a lack of political, military, and technological fusion. Historically, a strategic surprise is contextual; it is conditioned by the particular problem and its existential nature and the culture, time, weakness, geography and desperation of the protagonist. Nevertheless,the lack of strategic foresight and passivity in the erstwhile Indian context led Pakistan and China to repeatedly exploit the fault lines and off balance India by strategic military surprise. The key issue remained the lack of C5ISR capability, parochial single service outlook and lack of strategic envisioning in the absence of a national security strategy. The key challenge for the military thus remains '*pre-empting rather than reacting* 'to restore an adverse situation and *'denial rather than defence'* of its national territory. From a military point of view, military surprise creates spatial, temporal, moral and psychological dislocation

and responses thereto prove costlier besides national embarrassment. A repeated lesson repeatedly lost sight. The saviour has always been the prowess of our junior leadership and regimental system which too is being tinkered with in recent times by those having little idea of matters military.

The prevailing fragile situation on our disputed borders mandates an integrated C5ISR architecture to generate superior situational awareness leading to predictive battlespace dominance as part of our joint force capability. The recent joint force structures of Space, Cyber and Special Forces along with the raising of the Defence Space Agency (DSA), discussion on impending tri-service integrated theatre commands,and GoI space reforms beyond ISRO to establish the Indian Space Association (ISpA), Indian National Space Promotion and Authorization Centre (IN-SPACe), New Space India Limited (NSIL)are earnest steps in the right direction. Yet the effort remains sub optimal in empowering the joint force C5ISR capability holistically, otherwise marred by service silos and gaps in civil-military fusion.

Indian Joint C5ISR Capability Construct and Challenges

Joint C5ISR capability is a potent weapon as a tool to achieve battlespace asymmetry. This capability would not only pre-empt and deter an adversary but would also assist to generate favourable combat ratios in time and space, enabled by superior shared situational awareness and joint precision engagements. The desired outcome will be effective credible deterrence and force multiplication effect in battle. While some progress has been made in systems and data interoperability, the defence forces still lack a common joint C5ISR architecture that efficiently operates across all domains, multiple platforms and sensors seamlessly. The present system is also more focused on the need to know rather than the need to share. The existing challenges and inhibitors are multi-parentage, lack of integration, accountability and duplicity in the system. Besides, there is the challenge of existing platform-

centric focus, and desired net-centric synergy, along with stimulus to processing, exploitation, and dissemination methods. These challenges have resulted in a sub-optimal C5ISR grid with limited capability, capacity, coverage, connectivity and ability to overcome constraints of weather and terrain. Thus, the need is for enhanced richness, reach and interaction in our Joint C5ISR architecture both along the LC (Line of Control) and LAC (Line of Actual Control).Thus, it is important to understand the C5ISR fundamentals and generate a focused approach to its capability manifestation.

Key Fundamentals Joint C5ISR

The object of Joint C5ISR is to champion the concept of “need to share” over the concept of “read to know”. Its key imperatives thus entail:-

- C5ISR is a General Staff function that is command-led and staff executed. Thus, C5ISR must be led, not managed.
- C5ISR goal must adapt to address problem-centric requirements and not a resource-centric approach. The ultimate aim is sensors irrespective of organisation, shooters independent of platforms and decision-makers irrespective of geographical locations.
- Joint C5ISR must dilute inter-service lines and shun a compartmentalised rigid approach. C5ISR must be joint theatre specific in keeping with the terrain, weather and operational needs specific to a theatre requirement.
- ISR (Intelligence, Surveillance and Reconnaissance) must be addressed holistically with a single parentage and not the present culture of developing `I’, the `S’ and the `R’ in compartments with little synergy. The need is to transform from a loose confederation of separate specialists and

reporting chains into an integrated joint service enterprise with single parentage.

- The heart of the C5ISR or its jugular vein is the communication or networks. Pervasive and persistent C5ISR is only possible if there is pervasive and persistent communication with seamless interoperability.
- C5ISR will only be empowered if we shift from a platform-centric approach culture to a network-centric approach. The outcome will be a factor of networking sensors, decision-makers and shooters.

Joint C5ISR Capability Development Focus

The focus for an integrated and joint forceC5ISR capability manifestation must hone on the following:-

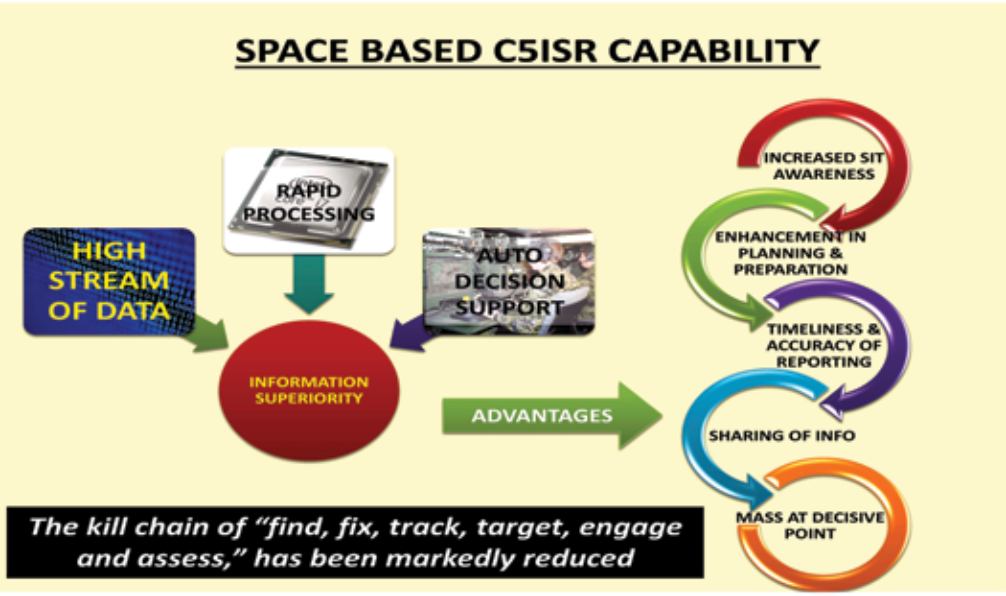
- **Critical Capability**. Persistent and pervasive, all-weather, all-terrain layered surveillance and fused intelligence for force multiplication effect at the cutting edge.
- **Capability Thrust**. Achieve seamless and secure information superiority across the battle space dovetailing state of the art technology with zero tolerance time.
- **Capability Mix Solutions**. A continuous multi-tiered, multi-domain, multi-intelligence and time-sensitive C5ISR grid.
- **Layered C5ISR and Networks.** Persistent, flexible, inter operable, affordable and survivable.
- **A Geo fused C5ISR data cloud.** With standard protocols at the apex level and data fusion centres for relevant needs at the lower level.

- **Multi-layered, secure, dynamic and robust communication backbone with terminal connectivity and plug n play concept** with a mix of both top-down and bottom-up approaches for Joint Service C5ISR optimization.
- **Human Capital.** Network agile, mission-orientedand focused C5ISR process mandates matching human resources, training policies and empowered structures. Above all, it requires a culture of jointness and tri-service synergy.

Space a Critical Enabler of Joint Force C5ISR Capability Generation

Space-based capability is an increasingly important enabler of the economic and military power of a nation. In the 21st century, Space power has evolved into a separate medium of warfare transforming from a combat support role to a warfighting domain. Thus, from the concept of '*Space Support'*, nations have graduated to the concept of *'Space Power'*.

India has shown progressive growth in its space capabilities both for civil and military applications to be a global space power. The concept of Pushpaka Vimanamin Indian mythology is akin to spacecraft and inter-planet astras or Space-based weapons, where guidance was through the mind of the commander. Interestingly, while the rocket was invented by the Chinese in 972 AD, it was the Indians (Tipu Sultan) who used it devastatingly for the first time against the British in the battle of Guntur in 1792. Since then, techno-military capabilities in Space have emerged as a major force multiplier and Space assets have become critically important in the security calculus of nations. Thus, while controlling the high ground had been a rule of warfare ever since the dawn of civilisation, the military advantages of this final frontier have become increasingly pronounced particularly in the field of C5ISR architecture.



Planning Imperatives for C5ISR Space Segment

Space-based sensors perform ISR that contribute to battle space awareness in all domains ranging from electro-optical, IR, SAR, and Hyperspectral to ELINT/COMINT, providing an opportunity to address a wide EM spectrum and provide inputs unhindered by weather, ambient conditions or operations on the ground. Satellite Constellations for C5ISR need to be based on a layered architecture with layers for persistent surveillance, broad area coverage and a high-resolution layer. The design characteristics of these layers need to ensure capability for both tactical and strategic C5ISR functions. Further, the integration should not be limited to just Space-based C5ISR systems but also corresponding air and surface-based systems because pursuing independent C5ISR capabilities would amount to defeating the basic concept.

The planning of this C5ISR Space segment should include:-

- Sub metric resolution for the High-Resolution layer and viable military resolutions for the broad area coverage and persistent surveillance layers.

- Varied local times of satellite passes.
- Inclined orbits for better coverage at certain latitudes.
- Number of constellations to ensure revisit capability to meet operational imperatives.
- Multi-sensor and joint service satellites to economise on numbers.
- Use of small satellite constellations to build in redundancy against adversary's counter-space operations.
- Develop a quick launch capability as part of the operationally responsive strategy with an aim to Launch on Demand (LoD) for critical areas in emergencies.

Space Based C5ISR Matrix

Space capabilities span all six warfighting functions, yet the most critical capability generation remains its C5ISR force multiplication effect. Its holistic capability generation matrix must ensure the mantra of - *"See the Battle space with Clarity, Communicate with Certainty, Navigate with Accuracy, Operate with Assurance, Acquire with Agility and Strike with Precision,".* These capabilities must manifest as under:-

- **Space Enabled Command and Control.**
  - Robust SATCOM and Space-Based ISR for full situational awareness of own forces and assets to facilitate distributed collaboration and planning among geographically dispersed elements.
  - Secure and Reliable wide-area SATCOM coverage for enabling battlefield commanders to exercise command over widely dispersed combat elements.

- **Space Based ISR Capability**.
  - Space platforms with EO / IR / SAR / hyperspectral / MTI surveillance and coverage between unsecured areas of responsibility, to give an unprecedented view of the battlefield. Generate ELINT, Multi/Hyperspectral Imagery and Dark Period Detection capability.
  - Develop Persistent surveillance, sub metric (0.1m) resolution, revisit every four hours, all-weather capability and enhanced repeat passes at varied timings. Develop strip instead of spot imaging.
  - Attain near real-time data dissemination with a demand to the delivery cycle of not more than four hours. A data relay system based on Geostationary satellites for quick transmission of acquired data from satellites to the ground earth stations with requisite bandwidth.
  - Operationally Responsive Space with enhanced focus on Launch on Demand(LOD) concept to supplement the present Launch on Schedule concept. Build Stockpile for short notice LOD to suit the operational environment.
  - Manning and Training – Develop Domain Specialisation with a mix of uniformed and civil specialists.
  - Need for high-resolution geo synchronous surveillance satellite for northern borders. It is critical to review the present orbital path and inclination for an optimised look in capability.
  - Move from service-specific satellites to Joint Military Satellites with dynamic sharing. Develop oceanic reconnaissance capability to meet the expanding area of interest and maritime reach.

- Develop Cluster of Satellite Capability as under:-

Satellite Class	Constellation Size	Capability per year	Remarks
ELINT cluster in one launch (300-400 kg each)	3 clusters of 3 satellites each	1 cluster of 3 satellites	Critical requirement – could be mounted with other payloads
EO / SAR EO-500 kg, SAR-1500 kg	12 satellites (6 SAR, 6 EO)	4 EO / SAR satellites	Critical for all-weather capability
LEO small satellites constellation (100-150 kg each)	24 small satellites	8 satellites	Complements dedicated ISR satellites

- **Manoeuvrability.**
  - Interoperable PNT system for precision timing and manoeuvre through threat sensor coverage gaps.
  - Near Space Platform ISR capabilities working in conjunction with integral UAVs to provide a virtual covering force to the operational commander.
  - Using Space SIGINT, ELINT and precision fire power with a manoeuvre to create a virtual high-speed lane through the battlefield.

- **Protection.**
  - Space assets to provide early detection of battlefield events, such as missile and rocket launches.
  - Tactical Space Effects to generate the form of spoofing or deceiving adversary intelligence-gathering satellites, denying communication access, disrupting or destroying adversary ground segment nodes.
  - Denying adversaries, the ability to use Space to

command assets and conduct ISR activities to protect information and decision-making superiority. This would include defensive and offensive space-based capability.

- Protection against cyber measures.

- **Precision Engagement.**
  - Future Space weapons capable of delivering precision attacks anywhere on the battlefield at short notice can be used to destroy hardened targets or even to create disruptive effects such as disabling urban power and information infrastructure grids.
  - Near Space capabilities to allow future combat systems to target adversaries deep into the battlefield. Potential targets can be engaged with conventional systems or battlefield lasers that may use the near Space platform as a repeater to redirect laser shots over the horizon.

Approach to Space Based C5ISR Capability Generation

Space is now the eyes, ears and voice of the modern military commander. The sovereignty and security of the nation will rest on the fact, of how it exercises Space control over the entire battle space. Future military Space operations must be treated with the same "developed-for-war" approach that today is applied to operations to joint force application. Space systems must be developed with readiness, sustainability, modernisation, and force structure in mind. Towards this end, an "Integrated Tri-Service Space Command" including functions of ballistic missile defence to meet the growing need of controlling cum exploiting Space assets is imperative. This structure should evolve Space strategies and "Joint Space Doctrine for Space Domination" that logically ties Space power theory, policy, and Space strategy together

and most importantly in a synergetic and joint operating environment.

The time has come to think about a focused institutionalised and time-stipulated approach to generating Space enabled military capabilities so that becoming a 'Space Power' does not remain a mere cliché. The Indian Armed Forces must, therefore:-

- Leverage Space operations and Space systems in all military operations with a focus on force enhancement and defensive Space control.
- Leverage current Space-based capabilities and maximize potential future Space activities.
- Articulate requirements to ensure fielded capabilities meet the needs of the Armed Forces.
- Institutionalise and train "Space Warriors" at the leadership and execution level.
- Organisational structures to exert influence in the national security Space community to achieve its vision.

The uppermost need is to integrate the intra and inter-service C5ISR capabilities. This would apply equally to *"Headware"* - doctrines, skills, training, people and processes; *"Software"* - GIS, data, automation and clouds; and *"Hardware"* - equipment, communication and infrastructure. A Joint C5ISR Philosophy essentially enabled by Space assets must be evolved to harness shared situational awareness blurring intra and inter-service compartments. The ownership must be taken by the newly founded Department of Military Affairs under the new CDS for a time-sensitive implementation. It should include the *'Joint C5ISR Doctrine'*, as an overarching framework, common data formats and data dictionary, common GIS with geo-referenced data, common coordinated digital maps and software, standard protocols, policies and procedures, as also joint encryption system moving towards quantum.

There is also a need for generating both threat-based theatre-specific *'joint problem statements'* by end users and simultaneously *'space technology capability demonstrators'* by space organisations, scientists and Private Industry as the drivers for C5ISR procurement. The requirement and desired capabilities must be sensitive to the operational environment viz weather, altitude, terrain and counter capabilities of the adversary. These must include surveillance challenges of border management, monitoring of infiltration, transgressions and intrusions. Additionally, they must forewarn any infrastructure development including depth areas leading to future capabilities, monitoring border training areas for a coherent picture of adversary's tactics, intentions and mobilisation plans, and shaping the battle space for Intelligence Preparation of Battlefield. Each theatre and sector must thus generate operational problem statements to be addressed by a focused and time-sensitive C5ISR capability development. Simultaneously while the space industry finds indigenous technological solutions to the above, they must be more proactive and invest in space R&D for next-generation military or dual-use technologies and space-based disruptive technologies to empower joint warfighters of the future.

The power of dual-use technology in Space and civil-military fusion for C5ISR must be harnessed to optimise national capabilities. The boundaries that separate civil and military space assets are getting blurred and most of the applications have dual-use capabilities. This mandates greater inter-play and joint participation between the government and commercial space agencies. With increasing private-sector participation and legislation cum reforms, the space industrial ecosystem in India is growing at a faster pace beyond the boundaries of ISRO. It thus provides an opportunity for the Indian Space sector to engage with the global space economy to maximise its gains and the potential of its strong capacity to build satellites and launch vehicles. The need is for greater support and hand holding of the private space sector and moving beyond an ISRO-centric model. The doctrinal imperative is

to harness this high ground with a whole of nation approach in terms of a *'National Defence Space Strategy'* to empower national security with an indigenous character. The key enablers for the future will be adequate funding, vibrant R&D for technology infusion, civil-military fusion, space diplomacy and exploiting open source intelligence.

Lessons from the Ukraine conflict have demonstrated the role played by private actors in monitoring the troop's movement and providing satellite imagery during the conflict. The commercial high-resolution satellite imagery provided by companies such as Planet and Maxar Technologies allowed unprecedented transparency to the West and in turn Ukraine. However, while commercial high-resolution optical imagery is available, all-weather SAR imagery is more limited and thus the importance of civil-military space fusion. The Ukraine war also highlighted the importance of developing an indigenous space access system while leveraging the global civil commercial sector.

Conclusion

Space-based C5ISR plays a critical role, not only in maintaining superior situational awareness but in conducting operations to prevail in today's war and fight to win future wars. However, the challenge remains in addressing the cultural, cognitive, doctrinal, fiscal and physical domains, to manifest Joint C5ISR into a time-sensitive indigenous desired capability.

India should presently adopt an integrated approach and continue to launch military and dual application satellites instead of present service specific or civil-oriented with enhanced military utilization under a declared 'Integrated Space Programme'. The focus should shift from defensive Space control missions with dedicated military Space assets and incrementally further build up indigenous offensive Space control and force application capabilities, both as a deterrent and a strategic capability. At the same time, India should collaborate with

other developed space power nations as part of ‘Space Diplomacy’ to develop niche disruptive technologies in pursuit of a futuristic space programme. Simultaneously, indigenization and R&D including private sector participation must get a stimulus. As India races into this new military frontier under ever expanding and perilous threat envelope, its trajectory must gain momentum with supporting doctrines, structures and capabilities. Space-based C5ISR is indeed the final frontier that India must conquest for the protection of its vital national interest.

Lt Gen A B Shivane, PVSM, AVSM, VSM (Retd), former DG Mechanised Forces and a Strike Corps Commander. The Officer is a defence analyst and prolife writer on matters military. He is presently Distinguished Fellow and occupying COAS Chair of Excellence at CLAWS.

111-124

C4ISR ARCHITECTURE FOR AN INTEGRATED AIR DEFENCE AND BMD- NECESSITY AND FEASIBILITY

Air Marshal Daljit Singh, PVSM, AVSM, VM (Retd)*

Introduction

Historically, technological developments have changed the way the wars have been fought. From dropping small bombs employing biplanes during early years of World War I, to the massive bomb loads of two tons dropped at night over London, by the German Zeppelins during the later period of the World War, the offensive strike capabilities have been advancing exponentially to conduct aerial attacks. During World War I, technology could not match the perceived strategic and operational concepts. With significant developments in aviation technology, radars, electronic navigation, propulsion systems and communication network, World War II saw massive improvement in bomber and fighter forces which delivered thousands of bombs during day and night, and which culminated in the employment of the first nuclear bomb on 06 August 1945 that struck the city of Hiroshima, killing nearly eighty thousand people.[1] To counter the air strikes, Air Defence Systems were developed by both the RAF and the Luftwaffe (German Air Force), which were based on radars, direction finding instruments, searchlights, anti-aircraft artillery, balloon barrages, visual observers and fighter aircraft. The first British integrated Air Defence network known as Chain Home (CH) or Dowding System was deployed along the east coast, with the Sector

Control Rooms established as Command and Control centers and they provided enmeshed data from diverse types of sensors and directed the 'shooters' for kills. The Luftwaffe also established an effective integrated air defence network with Operations Direction Centers to control the AAA, searchlights, and radar equipped fighter interceptors. Further technological improvements took place during the cold war period in propulsion technology, guidance systems and radar detection capabilities, and major nations like the erstwhile Soviet Union and the USA developed superior Surface to Air Missiles (SAM) like SAM II and Nike Hercules II. The first victim to SAM II missile during hot war was the F4 Phantom fighter being shot down on 24 Jul 1965, during the Vietnam War. The Americans lost 160 Phantoms to the SAM IIs by the end of 1965. This episode triggered the attack forces to develop Precision guided munitions (PGM) with standoff weapon delivery capability, Laser designated Pods (LDP), Anti-Radiation Missiles (ARM), Hunter-Killer Missions for Suppression of Enemy Air defences (SEAD) and Airborne Early warning and Control Systems (AEW&C). Electronic Warfare regained importance during this period to effectively counter Integrated Air defence network. In the meantime, significant development took place in the fields of cruise missiles and ballistic missiles which were first employed during World War II by the Germans as V1 and V2rockets, respectively. The V2 had an effective range of 350 km with one ton warhead, and circular error of probability (CEP) of 10 km. Nearly twenty thousand such rockets were launched with devastating effect on morale of the population. Since then, there have been massive improvements in the capabilities of the ballistic missiles and cruise missiles. They gained prominence as weapons of choice during the Gulf Wars, when the Allied Forces copiously employed cruise missiles and Iraq launched many Scud Missiles against Israel to lure other nations into the conflict. During the cold war period itself, when considerable number of nuclear capableballistic missiles were fielded by the Warsaw Pact nations, the Americans and other NATO allies, it

was evident that traditional sensors and shooters were incapable of effectively neutralising ballistic missiles, due to their high speed, low radar cross section (RCS), altitude and ranges. To ensure some level of deterrence, specific Ballistic Missile Defence Shields were developed by the erstwhile Soviet Union and the USA. With further technological advances in sensors, guidance technology and delivery accuracy, more theatre ballistic missiles and cruise missiles are now being employed as instruments of choice for attacks,as their employment does not cause own human attrition. During the ongoing Russian- Ukraine Conflict, conventional ballistic missiles have been used extensively by both sides. The extensive employment of ballistic missiles by the Iran backed Houthis during attacks on the UAE and Saudi Arabia in 2020, points towards this trend of weapon employment even by terrorist organisations. Many nations have, therefore, considered establishing 'Air and Missile Defence' infrastructure to optimise employment of resources, as the capabilities of AD sensors and shooters are improving and overlapping to tackle both air and missile threats. India also faces a serious threat of theatre missiles, cruise missiles, in addition to standoff precision guided munitions. A lot of developments are taking place in India to improve Air Defence and missile defence capabilities. It is, therefore, important to analyse whether it would be prudent to integrate these systems for their optimum employment and whether it would have any drawbacks

Indian Operational Environment

India faces two nuclear capable adversaries with significant arsenal of ballistic missiles, cruise missiles and modern fighters, capable of standoff PGM attacks. China has been developing advanced ballistic missiles with multiple independently targetable Re-entry Vehicle (MIRV) capability, maneuverable anti-ship missiles and hypersonic glide/cruise missiles. Its DF series of ballistic missiles has ranges to attack any target in India. The restructured PLARF Rocket Force has formidable

arsenal of ballistic and cruise missiles, and it continues to grow its inventory of road-mobile DF-26 intermediate range ballistic missiles (IRBMs).[2] PLAAF continues to increase its inventory of fourth generation fighters,and it has also fielded fifth generation J-20 stealth fighters and FC 31 stealth fighter is being developed for export as well as for Naval operations.[3] PLAAF intrusions in the Ladakh region continue off and on. Pakistan continues to engage India by asymmetric means, while it continues to modernise its Armed Forces. There have been significant developments in Pakistan to produce theatre ballistic missiles, cruise missiles and UCAVs.

Indian Air Defence Setup

The Government has entrusted IAF with the responsibility of the Air Defence of the Indian airspace. Therefore, control of all AD weapons is exercised by the IAF. Army has substantial number of ground based AD weapons to protect their war waging assets and specified Vital Areas/ Vital Points (VA/VP). Protection of Naval shore based assets is the responsibility of the IAF, while the AD protection of the assets at sea is the responsibility the Navy, which can be supplemented by the IAF early warning inputs. Organisationally, the IAF has five operational Commands, and each command has Air Defence Control Center (ADCC) which exercises control over all Air Defence activities within its area of responsibility (AOR). The IAF has a well-established, networked Integrated Air Command and Control System (IACCS) which is the nerve center for airspace management and weapons control. At present, nine IACCS Nodes are operational covering the entire Indian airspace[4]. Most of IAF radars are integrated with the IACCS to provide Composite Air picture of the air space. Civil radars and Airborne Warning and Control System aircraft (AWACS) are also integrated. The Army and Navy sensors are planned to be integrated with IACCS for exchange of information and control orders. The radar inputs are analysed and fused

to provide a composite air picture, which is shared with weapon control centers. There are many IACCS nodes spread over the entire nation that provide enough redundancy and resilience against attacks. The Surface to Air Guided Weapons (SAGW) are being integrated into the IACCS for effective and unambiguous target designation and execution. The IAF has been steadily inducting considerable number of modern radars with 4D detection capability. The venerable legacy THD 1955 long Range radars have been operating well and they are likely to be replaced by High Power Radars (HPR) that would have digital, active electronic steering array (AESA) technology with detection ranges of up to six hundred kilometers. There are also plans to induct 'Mountain Radars'[5]. Medium Power radars initially imported from Israel are now being manufactured in India as 'Arudhra'. The Indian made 'Rohini' 3D radar, Low Level Tactical Radar (LLTR) and low level light weight transportable radars are modern digital radars which are networked to the IACCS. The IAF has adopted multilayered Air Defence Systems concept to provide multiple tier protection with deployment of LRSAMS, MRSAMs medium range SAMs, Akash short Range SAMs, SPYDER QRSAMs, shoulder fired SAMs and anti-aircraft artillery. The IAF continues to employ the legacy SAM IIIs and SAM VIIIs effectively. The formidable S-400 SAMs are getting inducted, and the contract is signed to induct five Regiments comprising of 40 launchers, C2 elements and other support systems. The Indian Army has many legacy SAMs; however, MRSAM and Akash short range SAMS have been inducted and plans include additional MRSAMs, VSHORADS, Gun & Missile systems and AA Guns.

Indian BMD Project

Monitoring rapid developments of ballistic missiles by China, acquisition of M 11 SSMs by Pakistan, and threat by the Pakistani Foreign Secretary on 31 May 1999 to use 'any weapon' in the arsenal, during the Kargil Operations, prompted India to accelerate development of the Indian

Ballistic Missile Defence System.[6] BMD program also referred as Program AD (PGAD), was spearheaded by RCI, DRDO[7] and Defence Research and Development Laboratory (DRDL) developed the mission control software. [8] The components of the BMD include Long Range Tracking Radar (LRTR) (initially acquired from Israel as 'Green Pine' Radar and later produced indigenously), Multi-Functional Control Radar (MFCR), intercept missiles and Command and Control Centers[9]. Two types of interception missiles have been developed to undertake interception at various stages of ballistic trajectory. Prithvi AD (PAD) missile intercepts Ballistic missiles at exo-atmosphere at an altitude of 50-80 km and Advance Air Defence (AAD) missile is developed for interception in endo-atmosphere up to an altitude of 30 km. Phase 1 of development has been completed in April 2019, which provides capability to intercept ballistic missiles of 2000 km range.[10] Phase II of the development with more advanced missiles is under way to achieve the capability to intercept 5000 km range BMs. 'The deployed system would consist of many launch vehicles, radars, Launch Control Centres (LCC) and the Mission Control Centre (MCC). All these assets are geographically distributed and connected by a secure communication network.'[11] The MCC predicts the missile trajectory and designates the LCC to undertake interception. It would also calculate the interception probability and decide to launch more missiles to ensure success. 'IAF as the lead service for providing BMD protection of Delhi NCR has inducted one Multi-Function Fire Control Radar (MFCR) in NCR and one Long Range Tracking Radar (LRTR) is being deployed'[12]. These Radars are being operationalised in coordination with PGAD, DRDO and are being operated and maintained from internal IAF resources.[13] The Indian Naval Ship 'Dhruv' with capability to detect ballistic missiles and satellites, has been commissioned on 10 September 2021 as a maritime component of Anti-Ballistic missile detection system.[14]

Other Likely BMD Sensors

National Technical Research Organisation (NTRO) has been accorded sanction to procure two Very Long Range Tracking Radar (VLRTR) units as part of Missile monitoring System, to be manned by the IAF.[15] The systems are likely to have achieved the operational status by now. As the name suggests, these radars are likely to have much higher ballistic missile detection ranges.

High Altitude Pseudo Satellite System. Hindustan Aeronautics Ltd (HAL) has initiated a Project to develop High Altitude Pseudo Satellite System (HAPS), which would be solar powered, light weight airborne system, capable of staying afloat at an altitude of around seventy thousand feet for two months[16]. This system is perceived to bridge the gap between UAVs and satellite capabilities for surveillance and communications. This project commenced with funding by HAL and the project has now received the Government approval[17]. The system is likely to be developed in three to four years' time. The HAPS is a potential platform to detect ballistic missiles as well as other airborne objects. It could also be well exploited as communication relay station and Sigint sensor. The system could be integrated with IACCS to enhance overall situational awareness. NAL too has unveiled its own HAPS program in April 22, during Wings India Show at Hyderabad.

Space Based Sensors. In April 2019, the Government has sanctioned establishment of Defence Space Agency (DSA), to command the space assets of the Army, Navy, and Air Force, including the military's anti-satellite capability. The agency is also to formulate a strategy to protect India's interests in space, including addressing space-based threats.[18] Space provides excellent avenue for fielding sensors to detect ballistic missiles, hypersonic projectiles, and continuously gather Sigint data and geographical data. These inputs can be usefully integrated with other sensors to persistently track ballistic missiles and hypersonic glide or

propulsive vehicles. DRDO and private industries are keenly investing in space technologies, and we can see rapid progress in future, in this area.

Analysis

Recent operational trends indicate more employment of ballistic missiles, cruise missiles and attack UAVs, especially during the opening stage of confrontation. Even some terrorist organisations have employed these assets to create terror. China has significant arsenal of these missiles and dedicated Rocket Force has been organised to employ these weapons copiously. Pakistan has been developing cruise missiles and 'tactical ballistic missiles' to counter advancing Army formations. All modernising Air Forces like PLAAF and PAF have formidable bomber (PLAAF) and fighter force capable of attacking with standoff PGMs, Anti-Radiation Missiles (ARM) and air launched cruise missiles. Low level fighter attacks by overflying the target would be rare considering the lethality of the present AD systems. However, terminal AD assets must have the capability to neutralise the PGMs, cruise missiles and other types of munitions before they hit the target. Attack by small UAVs carrying explosives, against unprotected targets will increase, especially by rogue elements, as it was experienced at Jammu Airfield in Jun 2021. Effectiveness of AD Guns based CIWS against such attacks needs to be established before we go in for their massive induction.

India has well networked and integrated Air Defence set up, which has achieved good capability for continuous air surveillance and airspace management. It is a matter of time that all ground based weapons would also be integrated for improving the 'shooter cycle' and optimizing the C2 resources. The IACCS being indigenous system has great flexibility in upgrading the Command and control architecture and integrating future sensors, including the sensors from BMD, HAPS and NTRO systems. Manning of BMD and NTRO by IAF personnel makes it easier to integrate and operate these systems in a networked environment.

Future inductions of HPR, Mountain Radars and S-400 class of SAM systems with their embedded radars will significantly supplement the detection capability of ballistic and cruise missiles. S-400 class of missiles are also capable of intercepting ballistic missiles in endo-atmosphere regime and cruise missile, especially in 'self defence' mode. MRSAM radar may require some software change to detect ballistic missiles and engage them at closer ranges.

Deployment of Anti-ballistic missile system around NCR and other such Metropolitan cities would protect such VAs against only the ballistic missiles, whereas such VAs could also be attacked by other standoff PGMs, both air, and surface launched. It is, therefore, important to consider comprehensive protection of such VAs against all types of attacks. Other important VAs like military formations and other strategic targets like oil installations, nuclear forces and military industrial infrastructure are likely to be targeted by ballistic missiles. It would therefore be prudent to exploit additional capability of LRSAMs to provide integral AD protection including the missile defence. Net centricity can be well exploited to improve target detection and engagement capability of the Air and Missile Defence systems. No doubt, it would be impossible for any nation to protect all VA/VPs against all type of threats. There would be a need to consider VA protection priorities. Engagement of incoming threat must be quick and effective with prior approved SOPs and orders in place. There is no scope for lengthening the decision loop while engaging incoming known hostile threat. However, it would be important to share the filtered information with other agencies for their quicker follow up actions.

The nation must extract full capability of the expensive strategic assets that are generally available in limited numbers. While VLRTR types of sensors of NTRO are excellent assets to monitor specific activities, they are also capable assets to detect and provide better early warning against ballistic missile threat. 'Ownership' of such assets should not

impede in sharing crucial information that is available for other agencies to make use of. Net-centricity would enhance information sharing with relevant agencies in a secure and timely manner.

Space based assets will be crucial for enhancing space situational awareness and actionable intelligence, as further developments in sensor technology and secure satellite communications take place. Ballistic missile attack, monitoring hostile forces movement through Sigint sensors, geolocating targets, and mapping infrastructural developments and communications are some of the fields that can be best exploited by space based assets. It is important to share this valuable information with the dealing agencies in near real time. DSA would need to consider networking its Analysis Agency with MMS, IACCS and Service HQ operational Centers.

Rationalised Approach

Indigenous development of IACCS and MCC software has great advantage, as the source code is with Indian agencies, and it should be possible to modify the software as per operational requirements and reviewed Command and Control architecture. This will require close coordination between the agencies.

For providing comprehensive protection to NCR, and other designated strategic VAs, MCC, Space based data receiving Center and VLRTR radars should be integrated with IACCS. IACCS operation stations should be re-organised to have A&M NCR Director dealing with comprehensive protection of such VAs. With additional responsibility of Ballistic Missile defence, the IACCS should be renamed as Integrated Air and Space Command and Control System(IASCCS). 91N6E radar of S-400 SAM provides target data on all types of air threat including the ballistic missiles.[19] Inputs from BMD radars, S-400 target acquisition radar, NTRO VLRTR radars, Space satellites and HAPS (when

operational) should be fused to generate composite BM picture. The authority to engage all declared hostile targets should rest with ADCC through IACCS in its area of responsibility. Engagement process can be undertaken by MCC for anti-ballistic missiles and by Weapons Station of IACCS for other threats. Strategic Force Command (SFC) Operations Centre should receive filtered picture of the AMD and other air scenario for situational monitoring.

During peacetime, the control of the NTRO VLRTR type of sensors capable of ballistic missiles detection, should remain with NTRO. However, during crisis and heightened tension period, the control of the VLRTR should be exercised by the IAF through ADCC.

Air Force Network (AFNET) and Network for Spectrum (NFS) capabilities to service exchange of additional data should be examined and upgraded. The Data flow of the BMD and hypersonic attack vehicles should have priority over other data. If there is a constraint of data flow, dedicated network for BMD may be considered as a last resort.

IACCS should be the nodal agency to initiate ‘air raid alarm’ for civil administration to activate their plan.

To facilitate networking, all relevant sensors and shooters should have provision of overlaying software applications for RASP applications.

Likely Challenges

Organisationally, various sensors capable of BM detection are owned and maintained by different agencies. There would be difficulty faced in integrating these assets for operations. Directions from the ‘highest level’ should resolve this challenge, for ensuring maximum exploitation of these expensive national assets. Manning of NTRO and BMD assets by IAF personnel should facilitate integration and management of these assets smoothly.

Technically, networking and streamlined data flow would require further study to ascertain feasibility of streaming additional data with higher priority. Induction of the future sensors like HPR, HAPS and mountain radars should be networkable with IACCS. Full analysis of the network traffic, information priority and Command and Control software package, engagement algorithms would require major review and should be possible with active involvement of the operators and the scientists. Data fusion from sensors of different manufacturers would require interface and locally sourced algorithms which should be possible considering the mature status of the IACCS software.

Appointment of Committee of Experts dealing with the above mentioned challenges and clearly specified mandate should address the issues effectively.

Conclusion

Rapid developments in the fields of military technology have resulted in changes in operational concepts. Days of an attack aircraft overflying the target for weapon delivery are over. The fighters and bombers are now armed with standoff precision weapons capable of striking the targets from hundreds of kilometers. Ballistic missiles and cruise missiles have achieved credible delivery accuracy and they saturate and strain the defending forces without any fear of their own casualties. Recent conflicts indicate that future military engagements would involve significant employment of conventional Ballistic missiles and cruise missiles. Important VAs like NCR would require comprehensive AD protection as deployment of just the BMD would not protect NCR from other modes of aerial attack. The nations would require integrating all AD assets to ensure optimum and effective exploitation of the resources available. This would require effective and secure networking to provide fused data for employing the most suitable weapon in the shortest decision loop. Space based assets would provide valuable inputs in

detecting and engaging ballistic missiles and cruise missile. India has achieved success in developing an indigenous BMD system and its deployment to protect the NCR should have been approved. However, for comprehensive protection of such VAs, comprehensive air, and missile Defence is considered essential. The IAF has well established robust and resilient Integrated Air Command and Control System which can function as the C2 node for BMD and Air defence operations. S-400 SAM under induction has significant ballistic missile detection and interception capability. Data fusion from all assets capable of BM detection, including the sensors in space, would ensure comprehensive and wider BM defence capability. Organisational changes are required to exploit all assets of air and Missile Defence systems under one authority, for their optimum employment. Home developed software of BMD and IACCS can be best exploited to change the target engagement strategy and C2 architecture to match the operational imperatives. Time has come to surpass the organisational and technical impediments and be prepared for future war scenarios.

***Air Marshal Daljit Singh, PVSM, AVSM, VM (Retd),** is a former AOC-in-C, South Western Air Command and Assistant Chief of Air Staff (Air Defence) and Director General (Air Operations).

Endnotes

1 John Andreas Olsen, ed., A History of Air Warfare
(New Delhi: Vij Publications, 2010)

2 Department of Defense (2021), “Military and Security Developments involving People’s Republic of China”, p 51.

3 Ibid p 55.

4 Press Information Bureau 2014, “Major Achievements of Ministry of Defence from 2014 to Present”, Ministry of Defence, Government of India, https://archive.pib.gov.in/4YearsOfNDA/Comprehensive-Materials/defence.pdfaccessed on 09 Jul 2022.

5 Military History 2014, “List of Radars”, https://military-history.fandom.com/wiki/List_of_radars#Land-based_and_airborne accessed on 09 Jul 2022

6 Wikipedia, “Indian Ballistic Missile Defence Programme”, last modified on 23 August 2022, at 01:51, https://en.wikipedia.org/wiki/Indian_Ballistic_Missile_Defence_Programme

7 Defence Research and Development Organisation,2022, “Ballistic Missiles Defence (BMD) Programme”, Government of India, https://www.drdo.gov.in/ballistic-missile-defence-bmd-programme-pgad accessed on 07 Jul 2022.

8 Sparsh, 2021, “Understanding India’s Ballistic Missile Defence Programme”, Defence XP,https://www.defencexp.com/understanding-indias-ballistic-missile-defence-program/ accessed on 08 Jul 22.

9 Air Mshl Daljit Singh, “Developments in Air Defence Surveillance System”, AIR POWER Journal of Air Power and Space,7, No 2, (2022): 1:20

10 Sparsh, 2021, “Understanding India’s Ballistic Missile Defence Programme”, Defence XP,https://www.defencexp.com/understanding-indias-ballistic-missile-defence-program/ accessed on 08 Jul 22.

11 Ibid

12 Press Information Bureau 2014, “Major Achievements of Ministry of Defence from 2014 to Present”, Ministry of Defence, Government of India, https://archive.pib.gov.in/4YearsOfNDA/Comprehensive-Materials/defence.pdfaccessed on 09 Jul 2022.

13 Ibid

14 Inder Singh Bisht, 2021, India to Commission Missile-Tracking Vessel, The Defence Post, https://www.thedefensepost.com/2021/09/08/india-missile-tracking-vessel/ accessed on 09 Jul 2022

15 Press Information Bureau 2014, “Major Achievements of Ministry of Defence from 2014 to Present”, Ministry of Defence, Government of India, https://archive.pib.gov.in/4YearsOfNDA/Comprehensive-Materials/defence.pdfaccessed on 09 Jul 2022.

16 Akshay thakur, 2021, “HAL project to build pseudo satellite set to get approval for govt funds: Official”, The Indian Express, https://indianexpress.com/article/cities/bangalore/hal-project-pseudo-satellite-drone-defence-govt-funds-7519954/ accessed on 09 Jul 2022.

17 Raunak Kunde, 2022, “HAL’s HAPS Programme gets Government approval”, Indian Defence Research Wing, https://idrw.org/hals-haps-program-gets-government-approval/#:~:text=The%20public%20sector%20undertaking%20Hindustan%20Aeronautics%20Limited%20%28HAL%29,forces%20as%20confirmed%20by%20Defence%20Secretary%20Ajay%20Kumar. accessed on 09 Jul 2022.

18 Defense Space Research Agency (DSRO), 2019, Journals of India https://journalsofindia.com/defence-space-research-agencydsro/ accessed on 09 Jul 2022.

19 Ibid, p 11.

125-133

C^4I^2 SR IN AD THEATRE SETUP

Gp Capt RK Dhir (Retd)*

Introduction

Everything in today's world is happening at a great speed. Be it aircraft, weapons or computing, all are in a competition with themselves to outdo their recent performances. This has led to a complex problem of war fighting in an **electronically dense hostile environment** thus stretching and stressing every cell of the operator. Fully automated environment is a blessing, but a semi-automated one stretches every sinew of the decision maker. Conduct of C^4I^2SR operations in a smooth and seamless manner thus achieves greater importance as it endeavours to **integrate** the **machine logic** and the **human intelligence**. Success in such a complex environment is totally dependent upon **secure and redundant communication** backbone protected from enemy intrusions. Besides the above, **interoperability** between the **systems and manpower** is the game changer which is achievable only thru intense training sessions.

Confusion at overlap zones of responsibilities, similar weapons, defending same geographical area and **Fog of war** aggravate the already complex environment which can lead to fratricide and thus loss of clarity required in quick and correct decision making. This can lead to an entirely different outcome of war than envisaged. This gives rise to the requirements of an **Air Defence System** such as the **Theatre Command** for planning and conduct of Air Defence operations thus cutting down on the **delays** and **confusions** which would otherwise prevail due to many agencies operating within the same area.

This article deals with the urgent requirements of dealing with the enemy in a most professional and effective way. The requirements of joint training in simulated and live environment play a great role in sharpening the skills of operators and achieving a very high degree of team spirit.

Requirements

A joint **Tri-services** team needs to be put in place to carry out the following tasks in a time bound manner. This team should also have **retired officers** of all operational branches and should **not** be dominated by **any service/ branch**. Requirement of retired officers is a critical necessity owing to their vast experience and ability to express freely.

This team will **define Theatres** covering India and neighbouring countries and **assign** sensors and weapons accordingly. Their **locations** can also be defined based upon the existing threat thus ensuring optimal use of the weapons, no fratricide and safe conduct of operations by the three services. These can be subsequently changed depending upon the situation in that Theatre. Sufficient trained manpower as recommended by the team needs to be stationed in each theatre. No subsequent cutting down of the manpower should be done for the same settings/ task/ role of the Theatre.

Post commissioning, extensive **joint** theoretical and simulated/ live training on Conops, Weapon capabilities and their usage, integration with other elements of three services etc. needs to be carried out. The same trained lot, after they attain seniority should define new Conops besides revising old/ existing Conops.

Defining roles and tasks for three services needs to be clearly spelt out so as to have specific weapons for such roles. This would lead to clarity in the use of available weapons and reduce chances of multiple weapons on the same target situations.

Setting up of the Command and Control structure can be handled easily;

however, in a **highly dynamic scenario**, integration of **Radars, Imagary, Aircraft, Weapons** etc. to get ideal solutions taking into consideration their **capabilities, restrictions** imposed by various SOPs/ air and the actual situation on ground is a Herculean task which is likely to fail unless aided by state of the art technology like **Artificial Intelligence**.

To meet the challenges involved in airspace protection and reap the benefits of integrating the **sensors, communication** and **weapon systems**, most defence forces require field proven automated solution that support Tactical, Operational and Strategic level of operations.

The present system in use by the IAF is truly scalable and can be customised for use by the operators in a theatre command. This varies from **multi-level, multi-agency, multi-sensor, multi platform** and **multi C⁴I²SR centre** configuration down to a standalone C⁴I²SR centre (setup that is capable of operations either as a **sub-part** of the Theatre Command **OR** during progress of war, operating independently in areas which are cut-off from/ added to the existing Theatre AoR. The system is **interoperable** with other defense and civil systems and incorporates **state of the art algorithms, mathematical models** and **AI based techniques**. The details of their integration are already spelt out and the current system caters to the same.

Some of the prominent features of the desired system for exploitation by the operator at a Theatre operations centre are mentioned below:-

- **Sensor Integration.** All ground, sea, air and space based sensors of the armed forces/ civil spread far and wide shall be integrated at command centres using available communication networks and a common **Recognized Unambiguous** operating picture will be generated for the conduct of seamless operations.

- **Communication Integration**. The available communication of all forces located at different geographical locations shall

be integrated at the command centre using the available networks. The system can handle **voice and data** exchange with the operators at the remote ends.

- **Flight Plan System.** The flight plan system shall integrate the **civil** flight plan system and also provide the interface for entering the **Mil** flight plans. The system shall automatically perform **collision checks** on receipt of flight plans and also after the aircraft are airborne and suggest resolution in case of collision and also issue clearances to the flights.

- **Identification.** The system shall automatically identify aircraft by usage of **algorithms** on the basis of **Flight Plans**, **IFF, Target signatures** etc.

- **Surveillance System.** The system provides automatic surveillance features by continuously monitoring the airspace and provides alerts and corrections for aircraft likely to violate the existing rules/ SoP. Alerts on friendly aircraft transiting thru or operating over TBA and suitable weapon control orders will be generated for deployed weapon systems.

- **Danger Assessment**. The system continuously scans the airspace and automatically calculates the danger posed to protected assets from enemy platforms. Alerts are provided to the operators in real time.

- **Weapon Solution.** The threatening target is assessed to automatically suggest best suited weapon (Aircraft/ Missiles/ Guns) to neutralize the threat at the earliest. The system automatically generates **guidance commands** for friendly **Fighters** and **solutions** for the **Weapon systems** enabling them to intercept the hostile airborne objects.

- **Recovery Solution**. The system generates suitable

guidance commands for recovery of friendly aircraft based on their specific type/ condition.

- **Display System**. Display in **2D** and **3D** and a highly configurable **user friendly GUI** are the hallmarks of the Display system.

- **Record and Replay.** This module will provide a record of **synchronised** audio and video recordings. This is of great relevance in the analysis of incidents / accidents and effective training of the operators.

- **Simulation.** Simulator provides a **cost effective** means of near real-time training of the operational crew. State of the art simulator which can create scenarios based on enemy deployment of sensors, weapons etc. and using own forces against them will be the hallmark of effective training. The system will also provide analysis of the **operator actions**, **kill validation** etc.

- **Security.** The entire system is protected from **external threats** using multi layer security. **Defence-in-depth** measures of cyber security such as Access control, Data confidentiality, Data authentication, Integrity, Non-repudiation are critical features of the system. To meet these features cyber security technologies including biometric access control, end point security, system hardening, communication security, data encryption (including logs related to system and new versions) etc. will be used.

- **Database.** A robust and redundant database is the heart of the system and will provide seamless operations round the clock. The high end requirements are planned to be met by **resilient database design** having comprehensive industry-standard technologies like active-active clustering,

database auditing, database security for data at rest and data in transit, database firewall solutions and real time data replication solutions across distributed network.

- **Maintenance and Sensor Watch Planner.** This is tool which takes away the major time load of the operators involved in manual planning. It takes into consideration the time a sensor has operated / any restrictions defined, maintenance due, coverage required in a specific geographical area etc.

- **Inventory Status and Planning Tool.** The system will keep a track of various inventories such as weapons, fuel, oil, lubricants, ration, arms and ammunition etc. and provide advance alerts for procurement / replenishment of the same. Equipment hours used and remaining will help in planning their day to day usage.

Suggested AD Setup at Theatre Level

Following is the proposed setup at the Theatre level for seamless conduct of operations leading to subjugation of the enemy:-

- A Tri services war plan based on relevant Conops should be drafted for such an Air Def Theatre Command. It needs to define the roles and responsibilities of all elements within its AOR.

- The senior most Fighter Controller (Designated as the **Theatre AD Commander** is proposed since this is the **only** profession which is exposed to all aspects of **integration and exploitation** of sensors, weapons, flying operations etc.) in the Theatre AOR who should be the decision making authority under whom Tri-services assets should be placed. The **Theatre AD Commander** will be reporting to the CDS from whose office conduct of operations will be monitored

and controlled. Similarly all other Theatre Commands should also be controlled by the same authority for easy and quick co-ordination amongst all.

- Under the Theatre Commander AD needs to be placed one officer of each service (Designated as the **Deputy Theatre AD Commander** IA, IN and IAF). They will execute all orders given by the Theatre AD Commander using a customised S/W solution providing them with **assessment of Danger** and the **optimum Weapon solution** for neutralising the perceived threat. The operators will also have the facility of report generation, saving and replaying the events at their disposal. Physical safety and redundancy will also be the hallmark of the C2 centre.

- Under each of the Deputy Theatre AD Commanders will be multiple **warrant ranks**, each responsible for a defined number of weapons deployed in the field. The will pass **weapon control orders** and receive **acknowledgements** using encrypted data and voice channels. The entire communication will be in redundant mode so as to ensure NIL communication losses / delays.

Conclusion

The tremendous technological developments in the recent years has not only increased the lethality of the aircraft/ airborne threats but has also resulted in concurrent development of equally lethal weapons to counter the threat from such aircraft/ airborne threats. Such high speed and gap exploiting aircraft, operating over friendly **vulnerable areas** and **vulnerable points** provide minimal time for their **Detection, Identification, Interception** and **Destruction.**

Stealth technology, exploiting enemy **radar gaps** etc. reduces the detection time considerably; this, coupled with more accurate **Stand**

Off weapons further reduce the time available for their **identification**, **calculation of quantum of threat** and choosing **best suited weapon** for neutralising the threat. The situation is further aggravated when more than one service (Army, Navy or Air Force) is operating in the same theatre of war. Moreover, the new scenario wherein a war could only be limited to a specific geographical area with all other flying (civil aircraft) taking place as usual is bound to result in a massive strain on the Command and Control agencies as the co-ordination required for incident/ accident free operations while maintaining secrecy of the missions is of a very high order.

An ideal situation would hence be to have all the resources viz. Sensors, Visual means, Intelligence, Aircraft, UAVs, Weapons, Communication, Electronic Warfare elements etc., located within an **Area/ Theatre** under the command and control of a single agency to deal with the threat in an effective manner.

Another critical issue that needs immediate attention and redressal is the **delayed finalisation/ freezing** of requirements and **scope creep** that lead to extended timelines for roll out of the product when made by the Indian industry. Besides, this various **procedural** and other constraints result in slow acquisition (from foreign OEMs) thereby **impacting training** and **exploitation** of state of the art weapons and sensors. Thus need of the hour is to immediately address these issues particularly in the prevalent uncertain and hostile geo-political environment.

The only mantra is to have a Theatre command **manned** by highly trained and motivated operational staff as suggested before. It may seem impossible while it is being discussed, however, the only way forward is to form the same and have multiple scenarios being practised in a **simulated environment**. This has to followed by a **thorough analysis**

arriving at gaps and loopholes which are then translated into Conops, should be the way to move forward. Such an approach will be the most effective in operationalising the new concept of an Air Defence Theatre Command.

Gp Capt RK Dhir (Retd) *is a Category 'A' Fighter Controller who took PMR in 2017 after nearly 29 years in the IAF. Presently, he is serving as the AGM in Development and Engineering division of Network Centric Systems Strategic Business Unit of Bharat Electronics Limited.*

JOINT C4ISR AND FUTURE READY FORCE

Brig (Dr) Navjot Singh Bedi

Introduction

"War is but one of the ways of enforcing the political will of one nation upon another and is diplomacy by other means".

Since time immemorial, tribes and nations have waged wars and only the methods, means and morals of waging war have changed over a period of time. War fighting in olden times was a gentleman's business with strict rules of engagement being followed. However with the passage of time, these rules got diluted and attacks started being mounted at night and civilians, women, elderly & children also started being targeted. Over a period of times, wars saw tools and technology augmenting brawn and sheer brute force.

Rationale for Change & Imperatives to Usher in C4ISR

Organizations (including the Armed Forces) need to adopt certain aspects like radical adaptability, co-elevation, resilience and foresight, which are essential for an organisation to succeed in this new era. Radical Adaptability prompts an organisation to constantly anticipate change, reinterpret it, and transform through change. This concept is predictive, proactive and progressive, which is in line with the ethos of a *Future Ready Force* (**FRF**) as concepts of Inclusion, Agility, Resilience,

and Foresight are required to build agile combat teams. Future proofing & restructuring the Armed Forces and communicating the organisation's long-term purpose are important aspects for building a radically adaptable FRF. The pandemic showed that slow change can leave an organisation behind, thus radical adaptability may well be the survival practice of a modern day **FRF**. High performing teams go beyond cooperation; they need to operate in backdrop of a converged C4ISR backbone. Concept of co-elevating teamwork, wherein team members together create results that raise their capabilities as individuals, is a central aspect for Joint C4ISR & FRF; where synergised power of Integrated Tri Service team scan be leveraged.

Role of Technology & C4ISR in Future Conflicts

We are in the midst of a major technological transition and any conflict in future will see preponderance in use of technology to enhance C4ISR capabilities of the force. A *Future Ready Force* (**FRF**) needs to incorporate all emerging concepts of warfare which are technology predominant, essentially all-encompassing and impact the geostrategic, geo-economic and geopolitical domains. Though the pre-eminence of infantry and AFVs needs no justification on account of the need to have boots on ground, yet essential components which need to be factored are cyber, space, special operations, informational warfare, psychological operations, legal, electronic, electromagnetic, hybrid / asymmetric ops, drones, Unmanned Combat Aerial Vehicles (**UCAVs**) & autonomous weapons/ vehicles including drones. These elements would in some measure also need to be integrated with the infantry and AFVs, which may be required to operate in small cohesive teams, forming part of cohesive Integrated Battle Groups (**IBGs**), which is where Joint C4ISR will have a major role to play.

A ***FRF*** has now become imperative due to the tremendous spurt in technological growth, which includes both *Incremental &Disruptive*

Technologies. Emerging technologies in general denote significant technological developments that broach new territory in some significant way in their field. Examples of currently emerging technologies include IT, nanotechnology, biotechnology, cognitive science, robotics, and Artificial Intelligence (AI).[1] The present day war between Russia and Ukraine has cast an ominous shadow of doubt on the survivability of AFVs against the onslaught of Drones. This is another example of the innovative manner in which Drones have been used to not only enhance C4ISR but to also act as a potent kinetic kill platform.

A **FRF** is envisioned as a complex yet coherent force that will expand the operational scope and reach of a nation's strategic-military establishment. Such a force should ideally employ the concept of Multi Domain Warfare (**MDW**) through Joint C4ISR. Though there are many technologies which will drive these changes and which will play a major role in all future conflicts, yet from amongst these technologies, only few prominent ones which have a major role to play in shaping the **FRF** will be discussed. Space, Cyber, Communication, Nano Technology, Artificial Intelligence (AI), Robotics, Drones & UCAVs and the effect of these technologies, in shaping the **FRF** in the Indian sub-continent will be discussed.

Space. Space capability is being exploited mainly in the fields of communication, Positioning, Navigation, Timing (**PNT**), surveillance, various other space applications which have tremendous potential in enhancing C4ISR capabilities. Development of space exploitation capabilities and selective development of counter Space capability will be instrumental in enhancing national security. Being a scarce resource, C4ISR capabilities available in this segment will need to be shared by the three services, under the ageis of DCA, HQ IDS, thus reinforcing the importance of Joint C4ISR for a **FRF**.

Cyberspace. Cyberspace today is a complex environment involving underlying ICT infrastructure used by common citizens, social media,

businesses, government including military across the world, thus blurring boundaries in time and space. Cyberspace has acquired strategic position by virtue of its global reach and it's rapid integration into the social, political & economic discourse and framework. Malfunctioning or breakdown of a well-knit web may have serious implications on social well-being, economic and business interests of a Nation. Therefore optimal exploitation of Cyberspace is a prerequisite for a **FRF**.

Martin Ford, author of 'The Lights in the Tunnel: Automation, Accelerating Technology and the Economy of the Future',[2] ,states that as IT advances, machines[3] and software will exceed capability of workers to perform most routine jobs. As robotics & AI develop further, even many skilled jobs may be threatened. This is applicable & aptly true even in the context of a **FRF**, though the political compulsions of finding adequate job opportunities may slow down the process of replacing humans with robots.

Acronyms of Few Emerging Technologies Enhancing C4ISR

Most of these emerging technologies referred to for boosting Joint C4ISR capabilities for a **FRF** are not employed in isolation but in concert with two or three other such emerging technologies; thus a number of acronyms have come up and few of them are as listed below:-

- **NBIC**, an acronym for Nanotechnology, Biotechnology, IT and Cognitive science, is a term for emerging &converging technologies. It was introduced into public discourse through the publication of *Converging Technologies for Improving Human Performance*, a report sponsored in part by U.S. National Science Foundation.[4]
- **GNR** (Genetics, Nanotechnology & Robotics) also propounds the same concept & found mention in Bill Joy's article in 2000 on '*Why The Future Doesn't Need Us.*[5]

- "**GRIN**", for Genetic, Robotic, Information & Nano processes/ Nano-technology,[6] was first used by Journalist Joel Garreau in *Radical Evolution: The Promise & Peril of Enhancing Our Minds, Our Bodies& What It Means to Be Human.*

- "**GRAIN**", for Genetics, Robotics, AI and Nanotechnology[7] is used by Science journalist Douglas Mulhall in his book titled *Our Molecular Future: How Nanotechnology, Robotics, Genetics & AI Will Transform Our World uses* "

Convergence amongst these technologies is evident and is a critical element underwriting the Multi Domain Warfare (**MDW**) concept. However MDW will be feasible only in the backdrop of a converged C4ISR architecture, hence the same is imperative for a **FRF** which would be required to carry out MDW. This requires convergence between inter-organisational and military capabilities, across multiple domains and environments, both in time and space. These create windows of advantage that enable an FRF to maneuver from a position of advantage. In this article, an attempt has been made to list out certain niche technologies which empower any **FRF** to undertake MDW, in the backdrop of a converged / Joint C4ISR architecture.

The aspects of Space exploitation / threats, counter Space capabilities and of Cyber are very much a part of any FRF but being a domain in itself, as such these are not being deliberated upon further in this article.

This paper will primarily discuss the role played by three enabling technological domains ie *Nano Tech, AI& Robotics (to include Drones and UCAVs)*, in enabling and empowering C4ISR capabilities that a *FRF* would need. The role played by these enabling technological domains, in shaping Information Wars in the Indian Sub Continent in the age of MDW, supported by an enhanced Joint C4ISR will also be analyzed in subsequent paragraphs.

Nano Technology

Nano Technology is a science dealing with manipulating matter at molecular scale. Nano sized particles exhibit different properties, other than those exhibited by their bulk (matter) counterparts. In case of Nano particles the concepts of Quantum mechanics, interplay of Electro Magnetic forces & effects due to random molecular motion become more pronounced and relevant. Due to the inherent advantage derived from small size, Nanotechnology finds enormous scope in military applications ranging from Nano Fiber for camouflage & stealth, Body Armour, Nano Robotics, Nano drones, Armed Robots etc. Few such applications have been explained in subsequent paragraphs.

Nano Fibers for Structures and Body Suits.

- **Associated Technology**. The small size and inherent strength on account of Quantum mechanics, interplay of Electro Magnetic forces and other factors make Nano Fibers suitable for improved weaponry and body suits with enhanced strength. This facilitates preparation of intelligent fabric with Computer & ICT inter weaved into the fabric, which is especially useful for making 'Body Armour'. This type of body armour is light weight and can be made more intelligent by incorporation of Health Monitoring system with tagging and tracking facility, providing enhanced C4ISR and battle field transparency.

- **Role in Shaping Wars**. Our borders with our neighbors in the West and the North/ North East are such that there are large No of remote in-accessible areas where advance medical support is not easily available. This type of body suit permits remote diagnostics and management of health parameters & is a major technological breakthrough, as it

will reduce the logistical dependency on casualty evacuation. This will indirectly strengthen the tenability of our defenses in the Siachin Glacier. Whichever nation state is more technologically advanced will stand a better chance in exploiting the same.

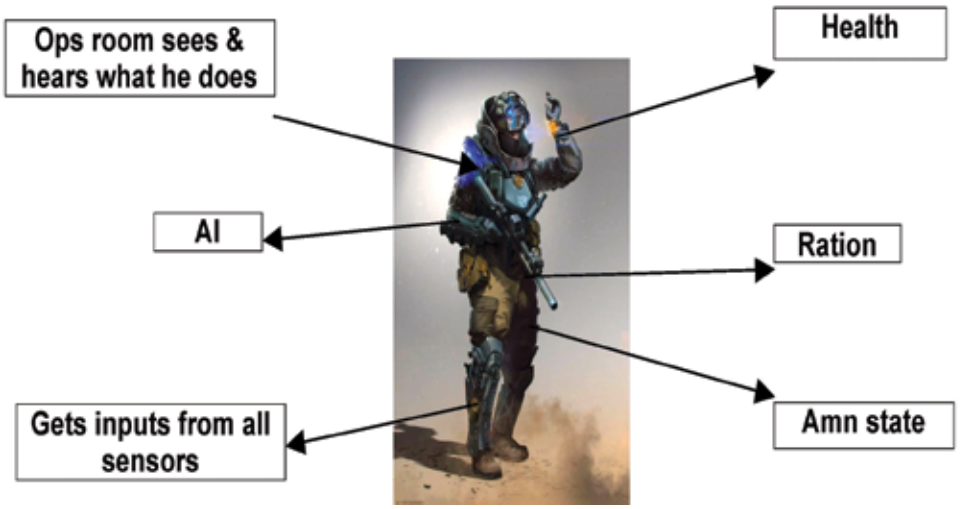


Fig 1:The Futuristic Soldier

The futuristic soldier shown in Fig 1 above will wear at least six sensors/ IP addresses; one each for monitoring the ration state, ammo state, health, for AI, to get inputs from all sensors and one to relay to the ops room, so that that the commander sitting there sees & hears what all he does. In one stroke the Joint C4ISR capabilities of Commanders are enhanced in the tactical domain, providing real time control of the operational situation and also empowering him in timely provisioning of requisite logistical support including medical assistance. Once an enhanced level of networking convergence is achieved, the input/ updates to the Commanders can even be automated.

Nano Robotics & It's Role in Enhancing C4ISR.

- **Associated Technology**. Due to the inherently small size, the Armed Robots can be made miniaturized, thus providing a smaller cross sectional area to be targeted, which in turn enhances their survivability and reliability, accuracy, lethality & efficiency on the battlefield. Such Nano Robots can also be employed in clusters and can be remote controlled, greatly enhancing the canvas of C4ISR.

- **Role in Shaping Wars**. This not only prevents loss of valuable human life in battlefield, but acts as a double edged weapon, especially in the context of porous borders. India has managed to fence it's large borders and put in place surveillance devices to monitor infiltration. However with the option of Nano Robots now available to the adversary also, preventing infiltration by Nano Robots, will be challenging and puts an additional strain on the surveillance grid. The side which is more technologically competent will be able to optimally employ these Nano Robots in the battlefield as they will be able to provide enhanced accuracy, lethality, efficiency, reliability & battle field transparency, leading to better Joint C4ISR.

Unmanned Air Surveillance.

- **Associated Technology**. UCAVs are being put to effective use by a No of developed nations to carry out precision strikes, with virtually no loss of life and nearly 99% assured success / strike rate and surveillance using **UAVs** is already creating waves. So acute is the problem that nations have developed and designed weapons to specifically target UCAVs and UAVs. However using Nano Technology now Nano Drones

having Nano processors can be made. These light weight and power efficient devices will provide their adversaries with a smaller cross sectional area to be targeted, which in turn makes them difficult to be detected and enhances their survivability and reliability.

- **Role in Shaping Wars**. UAVs and UCAVs are actually a game changer and they can partially bridge the divide between affluent nations which can afford latest 5th generation combat fighter aircraft/ MBTs and those which are unable to do so. Nano Drones can form a Smart/ Surveillance Dust, in which large number of Nano drones can form a decentralized net with computational and wireless communication capabilities. Thus due to the large numbers in the swarm, the disadvantage of limited computational power available in a single Nano Drone can also be overcome by the Smart / Surveillance Dust, comprising of a swarm of such miniature drones.

- The efficacy of drones has been demonstrated during the Army Day 2019 and has been seen in the recently concluded conflict between Armenia and Azerbaijan as well as in the ongoing war between Russia and Ukraine. These Drones can be used as air borne weapon platforms, as well as for surveillance, enhancing Joint C4ISR to the next level; in turn facilitating synergistic application of force within the three Armed Forces. This provides an asymmetric advantage to the side possessing drones and is an essential weapon platform in the arsenal of any ***FRF***.

Adaptive Camouflage & Stealth Coatings.

- **Associated Technology**. It's been correctly said that "you

can't shoot what you can't see." Using nanotechnology, the Electro – Chromatic properties of materials/ protective coatings can be altered dynamically to adapt to surroundings. Cloak Of Invisibility[8],[9] is made possible due to camouflage/ cloaking microscope tips at optical frequencies.

- **Role in Shaping Wars**. Nanotechnology enables ever increasing battle field transparency, making soldiers and weapon platforms invisible / difficult to detect. Thus the shooter or target platform is there but is not visible to the adversary, which enhances both it's lethality and survivability. This will be of immense use when the infantry would be required to operate in small cohesive teams forming part of cohesive Integrated Battle Groups (IBGs). It's applicability and utility for the Special Forces (SF) of the three Armed Forces (ie Para SF, MARCOS & GARUD Commandos) needs no elaboration and will in a way promote joint-manship.

Nano Sensors.

- **Associated Technology**. These are extremely small in size with high sensitivity and large surface area. They are capable of chip sensing, intelligent power savings & wireless communications, all of which makes them extremely useful for military usage and in enhancing the existing C4ISR envelope.

- **Role in Shaping Wars**. These are low cost & disposable, thus suitable for mass production and for deployment in remote, inaccessible areas, where retrieval, repair and recovery is either difficult or not economically/ tactically viable. Such terrain is found in plenty in the Indian Sub-continent. This attribute lends them suitable for various

Military Applications, few of which are as listed below:-

- Bio Chemical sensors for detecting NBC activity.
- Integration with Body Suite for Health Monitoring.
- Battle field surveillance.
- Forming Wireless Nano Sensor Networks comprising of large number of Nano Sensors operating in cohesion to cover large area's.
- Intrusion detection along critical gaps and at vital installations.

Nano Biotechnology.

- **Associated Technology**. Nano Biotechnology incorporates diagnosis and administration of drugs and is especially relevant for wounded soldiers using Nano Sensors. Nano Sensors embedded body suits permits remote diagnostics and management of health parameters & are generally used in remote inaccessible areas where advance medical support is not easily available.
- **Role in Shaping Wars**. Remote monitoring of soldiers health to maintain peak levels during operations is important and is possible due to Nano Biotechnology aided by Nano Sensors. This is especially useful in case of troops deployed in remote, inaccessible areas, where on call medical evacuation is either difficult or not feasible/ tactically viable. Adoption of this technology could give a fillip to the operations being conducted in the North and North East and serves as a uniform parameter/ platform to render medical support to the personnel of the three Armed Forces.

Artificial Intelligence (AI)

AI is intelligence demonstrated by machines in contrast to natural intelligence displayed by humans & other animals. In AI a machine mimics “cognitive” functions that humans associate with other human minds, such as “learning” & “problem solving. Certain prominent traits / capabilities that researchers expect an intelligent system to display are:-

- Reasoning, problem solving
- Knowledge representation
- Planning
- Learning
- Natural language processing
- Perception
- Motion and manipulation
- Social intelligence
- General intelligence

Associated Technology and Tools of AI. Many AI problems can be solved by intelligently searching through possible solutions, however AI automates this process through iterative learning. The logical proof can be viewed as searching for a path that leads from premises to conclusions, where each step is the application of an inference rule. Logic is used for knowledge representation and problem solving. The decision tree is perhaps the most widely used machine learning algorithm. Neural networks, or neural nets, were inspired by the architecture of neurons in the human brain and have simply automated an existing time tested physiological function.

Applications of AI. High-profile examples of AI include autonomous vehicles, medical diagnosis, creating art, proving mathematical theorems, playing games, search engines, online assistants (such

as Siri), image recognition in photographs, spam filtering, prediction of judicial decisions and targeting online advertisements. With social media sites overtaking TV as a source for news and news organisations increasingly reliant on social media platforms for generating distribution, major publishers now use AI technology to post stories more effectively and generate higher volumes of traffic. This provides ample scope for effective utilisation for IW, strategic communication, perception management and to also shape perceptions.

Role in Shaping Wars. Autonomous vehicles ie drones and self-driving cars can be effectively used for surveillance and bomb disposal tasks. AI can facilitate remote medical diagnosis at inaccessible high altitude locations and can help in solving mathematical problems which are a key in cracking cryptographic codes. Wargames, search engines especially programmed for military use, image recognition in photographs, prediction of strategic/tactical decisions by the adversary are some other areas where AI can play a major role. The predictive decision making dramatically shortens the OODA loop, enhancing C4ISR. AI can also be used to shape the environment by generating content and posting stories more effectively over various social media platforms, in order to generate favourable opinion for the Armed Forces and for the nation. AI being ubiquitous to the colour of the uniform, is a great enabler of Tri Service synergy, thus enhancing Joint C4ISR.

Winds of Change. Roles in IT companies that were typically assigned to employees with over 10 years of experience—the mid-level bracket—are now going to machines. For example, Capgemini is using IBM's cognitive consulting tool *Watson*, to assign people to projects, while Infosys is building a machine-learning platform that will help project managers take decisions to make better trade-offs between the number of people needed for a project and the timeline for completion. Such a transition can be expected to take place in the Armed Forces also where the background data / facts and figures would be prepared and

presented by AI enabled machines and put up to the commander for his decision. The training imparted to various staff officers would need to be restructured accordingly. Possibly certain mundane aspects of the execution could also devolve down to such machines. In the Indian Sub-Continent all major nations are going into digitisation in a big way and it is but natural that the transformation in the military will also take place accordingly on these lines. This change will be implemented uniformly across the three services and having a Joint C4ISR will go a long way in ushering in this change.

Robotics

Associated Technology. Robotics is an interdisciplinary branch of engineering and science that deals with the design, construction, operation, and use of robots, as well as computer systems for their control, sensory feedback, and information processing. These technologies are used to develop machines that can substitute for humans and replicate human actions. Many of today's robots are inspired by nature, contributing to the field of bio-inspired robotics.

Role in Shaping Wars. Robots are ideally suited for military applications and are being used in dangerous environments (including but not limited to bomb detection & deactivation), manufacturing processes and environments where humans cannot survive. Robots are suited for operating in an NBC/ NBC prone environment, where precision measurement / action is required and where it is not advisable for humans cannot to operate. The Indian Sub-Continent and it's immediate neighborhood comprises of possibly the largest concentration of both nuclear weapon capable nation states and those that are a victim of terrorist activities; this region thus has ample scope of employing this technology, in the backdrop of Joint C4ISR.

- **Robotic Surgery**[10][11][12] can relive surgeons to perform other

life saving tasks / supervise robotic surgery. This is a boon for military applications as there is always a requirement of (and a shortage of) skilled medical specialists in the forward areas.

- **Exo - Skeletons** are an extension of robotics with mil applications and may eventually reduce the need for Armoured Fighting Vehicles (**AFVs**), as each soldier will be an intelligent Armoured Fighting platform. This is a boon for militaries constrained by shrinking defence budgets. Since time immemorial, armies created obstacles to separate the mounted cavalry from the foot infantry & subsequently to separate the AFVs from the infantry, giving rise to the Ditch cum Bundh (**DCB**) canal defence system. The Exoskeletons, powered by Joint C4ISR, can help achieve the synergy of infantry and armour, which has been the challenge all armies have grappled with.

- **Powered Exoskeleton**[13] will make feasible Future Force Warrior (like Iron-man). This will provide a solution for heavy lifting and for paralysis / muscle related diseases and possibly a Human Universal Load Carrier. **Swarm Robotics**[14] will also be possible due to swarm intelligence, autonomous robotics, nanorobotics, particle swarm optimization, multi-agent systems and behaviour based robotics. All this will need to backed up with a robust Tri Service communication network, eventually resulting in enhanced Joint C4ISR.

Artificial Intelligence (AI) & Robotics

Convergence of both AI & Robotics will result in creation of AI robots. If the utility factor of both AI & Robotics is (say 'x'), then the utility factor of an AI Robot will not be twice 'x'; rather it would be 'x' square. Likewise if

Nano-technology was to be combined with AI & Robotics then we would end up with AI Nanobot, with an extremely high utility factor. The military applications and employability of such an empowered weapon platform are endless and are limited only by imagination. Smart manufacturing represents a leap forward from traditional automation to fully connected and flexible systems. The industry needs to embrace the challenges and opportunities of this new era and the FRF should readily adopt it.

Pitfalls of AI and Robotics

The world leaders are seized of how robotics, AI, and IoT are being adopted and how they will transform the world. It however needs to be correctly understood what would be the impact on history of self-learning machines[15] ie machines that acquired knowledge by processes particular to themselves and applied that knowledge to ends for which there may be no category of human understanding. Would these machines learn to communicate with one another? How would choices be made among emerging options? Mankind is at the edge of a new phase of human history where the situation to embrace technologies of MDW seems to be incomprehensible and even awe-inspiring to us. However any FRF would need to take the leap of faith and embrace these technologies, eventually enhancing Joint C4ISR.

Responsive 5G Backbone Communications

In order to make all the above attributes a reality, there is a need to have in place a responsive backbone communications grid with adequate bandwidth, low latency, a very high state of reliability and enhanced computing power at the edges. All this can be provided by a Military IoT(or MIOT) powered by 5G backbone communication grid, facilitating Joint C4ISR. The Armed Forces already have a strategic Tri Services Communication network and Project Network for Spectrum (NFS) is in the process of being rolled out. These will greatly enhance the Joint

C4ISR capabilities of Defence, ushering in synergy within the three Armed Forces, by way of a common applications riding over a converged network.

Conclusion

When considered in its abstract form, the FRF will wage wars using the MDW concept which is intended to be an all arms and all capabilities affair. The changing character of warfare will entail embracing this concept, which appears to be designed to degrade the deterrent potential of an anti-access system, and to render ineffective its kill-chain. The traditional approach followed by armies the world over is to neutralise a defender's anti-access system with overwhelming force. AFRF adopting the MDW will seek to selectively target, in a bid to degrade and/ or destroy - key capabilities of anti-access system. All the technologies listed above in this paper enable this desired end state. By leveraging these technologies, the FRF will not only drastically shorten the OODA loop but will also usher in synergetic application of Joint C4ISR, which will prove to be the battle winning factor in all future wars.

To quote Vice Admiral (Retd) Arthur K. Cebrowski of the U.S. Navy, and John J. Garstka,[16] at the turn of a millennium we are driven to a new era in warfare. Today there are 4 Billion Internet users, 3.8 Billion active mobile internet users and 8 Billion IOT Devices in the world. India's national stakes are huge in global cyber space, thus implying it's stakes in AI, Nano technology, Robotics and their consequent affect in MDW in shaping the Information Wars in the Indian Sub-Continent. There is thus a pressing need for a suitably equipped technology savvy Joint C4ISR enabled FRF to be in place.

There are no binding laws on cyber space governance and the other dimensions ie AI, Nano- Technology and Robotics are as yet "Global Commons" and uncharted territory. We are going through a fundamental

shift from platform-centric warfare to Network-Centric Warfare (**NCW**), which is as resilient as the concept of unrestricted warfare, which a FRF will need to imbibe.

C4ISR exploitation & MDW are the next important development in waging war and a FRF should be geared up to embrace the same. Multi-Domain Battle requires converging inter organisational and military, as well as lethal and nonlethal capabilities, across multiple domains and environments in time and space. This creates windows of opportunity that enable the FRF to gain a position of advantage. A beginning in this direction has been made by ushering in the concept of Integrated Theatre Commands (ITCs) & IBGs. These structures need to be fleshed out with a FRF which is effectively able to leverage the latest technology to optimally exploit C4ISR.

The domains of MDW include, but are not limited to, the geophysical and electromagnetic categories, leading to unrestricted warfare, which any FRF will be required to grapple with. A FRF employing MDW is the future and is thus likely to have a major effect in shaping the Information Wars in the Indian Sub-Continent. The importance of making the correct strategic choices to adapt or even survive in such changing ecosystems[17] is thus important and it is imperative to usher in a FRF which will effectively leverage various technological attributes to enhance C4ISR.

***Brig (Dr) Navjot Singh Bedi**, is a Brig PMO (DCN) and Commander DCA, New Delhi.

Bibliography

1. "Artificial Intelligence in Military Operations: Technology and Ethics Indian Perspective", By Lt Gen RS Panwar, AVSM, SM, VSM, PhD (Retd) Mar 2019.
2. "NCW: Concept &Challenges", Army War College Journal, Winter 2015.
3. Army War College article: "Principles of Warfare on Network-Centric Battlefield".
4. Excerts from the talk on Information Assurance, delivered by Charles Perrow, in the National Defense University, in May 2003.

Endnotes

1 Other examples of developments described as "Emerging Technologies" can be found at- O'Reilly Emerging Technology Conference 2008.

2. Bill Joy, 2000, "Why the future doesn't need us". Retrieved 14 November 2005.
3. Martin Ford, 2011, "Machine Learning: A Job Killer?"
4. Martin Ford, 2009, "Will Automation Lead to Economic Collapse?"
5. Mihail C. Roco and William Sims Brainbridge, eds. Converging Technologies for Improving Human Performance. (Virginia: Springer, 2002) 1-4020-1254-3.
6. Joel Garreau, Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies — and What It Means to Be Human (Crown, 2005). Doubleday. 0-385-50965-0.
7. Douglas Mulhall, Our Molecular Future: How Nano technology, Robotics, Genetics and Artificial Intelligence Will Transform Our World (Amherst, NY: 2002). Prometheus Books. 1-57392-992-1.
8. Rachel Kaufman, 2011. "New Invisibility Cloak Closer to Working "Magic". National Geographic News. Retrieved 4 February 2011.
9. "Breakthrough in bid to create 'invisibility cloak' as 3D object is made to vanish for first time". Daily Mail. 26 January 2012. Retrieved 3 March 2012.
10. "Doctors grapple with the value of robotic surgery". Houston Chronicle. 16 September 2011. Retrieved 24 December 2011.
11. "Robotic surgery making inroads in many medical procedures". The Jakarta Post, 8 March 2011. Retrieved 24 December 2011.
12. "Doctors Perform First Fully Robotic Surgery". PC World. 21 October 2010. Retrieved 24 December 2011.
13. Christopher Mims, 2009. "Exoskeletons Give New Life to Legs". Scientific American. Retrieved 21 April 2009.
14. "Riders on a swarm". The Economist. 12 August 2010. Retrieved 21 April 2011.
15. Henry Kissinger, 2018, "How the Enlightenment Ends", The Atlantic Journal, https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/ , accessed 09 August 2022.
16. Vice Admiral Arthur K. Cebrowski, and John H. Garstka,1998, "Network-Centric Warfare-Its Origin and Future", Volume 124/1/1,139, https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future, accessed on 11 June 2022.
17. James F. Moore, "The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems," Harper Business, 1996.

153-170

C4ISR SET-UP IN MARITIME DOMAIN EXISTING SYSTEMS, CHALLENGES, PATHWAYS FOR FUTURISTIC WARFARE PREPAREDNESS

Captain (IN) Kamlesh K Agnihotri (Retd)*

Introduction

Modern maritime warfare is characterised by stand-off engagements with increasingly versatile precision-guided weapons, which rely heavily on integrated electronic systems. Technological advancements in military systems and advantages provided by the Information Age have brought about a revolution in military affairs (RMA). In such a technologically catalysed environment featuring increasingly capable weapon and sensor systems, the initiative in naval warfare will rest with the side which can act faster and respond quicker than the adversary by shortening the Information-Decision-Action (IDA) cycle.[1]

In order to measure up to this aspect of modern warfare, the command and control architecture of a Force, duly supported by the communication networks– which in turn, are built on the increasingly powerful computer systems – would be the key determinant factor between winning and losing a war/conflict. All these together form the first side of a proverbial coin – termed as 'C4' in short – and remain at the core of all operational naval activities.

The building of an efficient maritime domain awareness (MDA) grid

to facilitate quick and correct decision-making by the 'Command and Control' hierarchy forms the other side of that coin. The effectiveness of such MDA effort in providing vital actionable inputs is predicated on the Intelligence, surveillance and reconnaissance infrastructure, spread, connectivity and their exploitation capabilities – termed as 'ISR' in short. The complementary aspects of both, viz. the 'C4' and 'ISR – termed together as C4ISR –when exercised synergistically across vast seascape have brought about an essential transformation in modern war-fighting.

The Indian Navy does acknowledge the immense advantages that could accrue in adopting this RMA and has taken proactive steps in incorporating its constituents within its combat preparedness strategy. The constant and focused effort of the Indian Navy in translating the all-encompassing Network Centric Warfare (NCW) into full operational capability has started to bear good results. The Navy has ensured that a wide range of operational activities, spread across all dimensions and vast areas, are controlled and coordinated through secure and efficient maritime C4ISR network. This Paper seeks to take stock of existing C4ISR structure in the maritime domain; analyse the technological, organisational, functional, cultural and procedural challenges that need to be addressed, and explore the possible and ways forward to meet the requirements of futuristic warfare.

Understanding C4ISR

At the outset, C4ISR is expanded as Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance. 'Command' as a concept is the exercise of authority and direction over forces assigned, by an individual so designated, for the accomplishment of a mission or task. 'Control' on the other hand, is the process through which 'Command' is exercised by the Commander; and involves the activities for organising, directing and coordinating the

given forces. C2 structures enable individuals to accomplish missions that require collective skills and energies. Its elements span all domains of warfare – physical, informational, cognitive and social.

Effective all-domain 'Communications' and 'Computerisation' are critical enablers of Maritime Command and Control (C2), particularly for the conduct of naval operations in distant waters and for prolonged durations. The addition of these two integral components has led to the acronym of C4 (Command, Control, Communications and Computers). The hierarchies of Maritime C2 correspond to the levels of maritime operations. These could either be overall C2, operational C2 or tactical C2, as per the demands of the situation.[2]

ISR activities form the key ingredients for achievement of maritime domain awareness (MDA); and encompass the process of integrating the intelligence process with surveillance and reconnaissance, in order to improve a Commander's situational awareness and assist in his decision making. Surveillance involves the systematic observation of a defined area of interest by various means – visual, electronic or photographic. Reconnaissance also involves the similar activities to collect combat information; the difference being related to time and specificity. Surveillance is a more prolonged and deliberate activity; while reconnaissance is generally conducted in a limited time frame with an aim to retrieve specific information. The objective of both activities is to locate and identify a target at longer ranges with sufficient confidence, so as to enable standoff engagement without collateral damage.

The combat information collected by surveillance and reconnaissance effort is analysed, evaluated, compared with historical data, and fused with inputs available from other sources. The end-product, relevant to the prosecution of a mission then becomes intelligence, and is passed on to the decision-makers.

Existing C4ISR Structure in The Maritime Domain

The scale and scope of the C4ISR has to be commensurate to the spread of area which has to be covered. In addition, the war-waging capabilities of the adversary, which define the extent of the 'threat in being' must be considered. It therefore, becomes imperative to assess the characteristics of the domain in which the Indian maritime C4ISR endeavour has to play out.

India's Maritime Military Environment

India has been endowed with a huge maritime area where its Exclusive Economic Zone (EEZ) extends to about two million square kilometers. The oceanic environment has also become a multi-dimensional battle space, with space and cyber-space domains getting increasingly integrated with the traditional surface, under water and aerial dimensions – in which naval forces generally operate. The presence of neutral shipping in the sea area further confuses the maritime picture, which necessitates enhanced ISR effort. The near-permanent naval presence of extra-regional powers in the primary areas of India's maritime interest, makes the MDA picture even more complicated. These factors affect all facets of maritime warfare, be it surveillance, localisation, classification, targeting and weapon delivery.

Current Indian Maritime C4ISR capabilities

Since the maritime medium comprises interconnected oceans without fixed boundaries and inseparable borders, and it is simply impossible for a single State to cover the entire oceanic space; India – like other countries – has defined its maritime areas of interest for ensuring better coverage and management of C4ISR effort. India's primary maritime areas of interest broadly span the maritime zones of India, the Arabian Sea, the Bay of Bengal, the Persian Gulf, principal international sea

lanes (ISLs) crossing the IOR, and the choke points leading to/from the Indian Ocean via these choke points.[3]

The Current Indian Maritime ISR capabilities revolve around the need to keep continuous watch in its primary maritime areas of interest. The first principle is to establish a baseline datum of the level of maritime activities by various players in the domain over a period of time, which would be considered as normal. The aim is to readily discern any deviation from this normal pattern of activities. The means to achieve this objective are grouped into following categories:-

- **Static Surveillance**. Coastal surveillance radars and automatic identification system (AIS) receivers are mainly employed on the Indian coastline, outlying islands and offshore installations. Additionally, radars at major ports as part of the Vessel Traffic Management System (VTMS), monitor and manage the ships approaching respective harbours. These static surveillance systems provide active information on vessels operating in their vicinity and feed into the overall MDA development process.

- **Dynamic Surveillance**. This is undertaken by deployment of the Indian Navyand Coast Guard assets in Indian areas of maritime interest. These assets comprise ships and their sensors, maritime patrol aircraft, helicopters, unmanned aerial vehicles (UAVs) and even submarines, in some cases.

- **Space Based Surveillance**. ISR is also facilitated by use of space based AIS systems, with the Indian Navy having integrated this technology towards MDA development., such surveillance can additionally be expanded by fitting satellite transponders on smaller ships, including fishing vessels. Space-based assets can also be used for imaging by Synthetic Aperture Radars (SAR), Electro-Optic (EO) and

Electronic Intelligence (ELINT) sensors.

- **Position Reporting Systems**. Merchant shipsat high seas and those approaching Indian ports / islands report their positions by manual or automatic means, under voluntary and mandatory mechanisms. The information from these systems is also linked and correlated to MDA development process.

- **Air Domain Awareness Processes**. Air Domain Awareness (ADA) is a vital component of maritime situational awareness. Technologies such as Automatic Dependent Surveillance-Broadcast (ADS-B) and e-flight plans are integrated into the MDA network architecture. Integration of the Indian Navy's operational network with that of the Indian Air Force is planned so as to enable feeding of the Air Defence Identification Zone (ADIZ) picture in the national ISR grid.

- **Intelligence collection and data analysis**. Measures for analysis of the information are also vital to develop a common understanding of the maritime operating environment. Intelligence gathering and sharing on continuous basis between intelligence agencies is also being tried for developing effective MDA.

- **International Maritime Information Exchange**. India has signed 'White Shipping' agreement with 22 countries for sharing information on movement of their ships, so as togenerate a comprehensive regional and global maritime picture.[4] The Indian Navy's Merchant Ship Information System (MSIS) enables the collation of white shipping information from various sources. The Indian Navy's Information Fusion Centre–Indian Ocean Region (IFC–IOR) which was established in December 2018, is presently

engaged in stellar collaborative venture with global stakeholders, with liaison officers from 10 countries working and training together.[5]

Challenges in Effective Implementation of C4ISR

C4ISR aims at increasing the combat power of a force by networking the entire command and control chain right down to the unit level, through all-domain communication systems. C4ISR systems strive to share information, build shared domain awareness and ultimately achieve complete hierarchal synchronisation. But the real importance of C4ISR lies in how the military uses its constituents to shorten the Information, Decision, Action (IDA) cycle to gain operational advantage over the adversary.

However, the changing technology and newer concepts of operations should not allow the Command chain to digress unduly from the time-tested – and still very much relevant – Principles of War. The Adoption of C4ISR concepts and technology will not always ensure getting the better of the adversary in modern warfare. The implementation and conduct of C4ISR activities are also fraught with challenges and pitfalls, which the entire command and control chain must understand and consider whilst conducting military operations. The succeeding paragraphs bring out some of these technological, organisational, functional, cultural and procedural challenges and pitfalls related to the execution ofC4ISR effort.

Technological Challenges

Developmental Challenges. Communication and ISR systems are expensive because of the costs involved in research, development and procurement. The development of C4ISR systems in the backdrop of rapid obsolescence in the field of information and communication

technology (ICT), will remain anall-timechallenge. The high costs of replacing legacy combat systems with C4ISR enabled ones also makes total transformation economically unviable. Given these constraints, a modular development cycle using indigenous technology, with open inter operable standards and protocols should be attempted to enable progressive upgrades and stepwise refinement.

Maintaining the Technological Edge. While it is posited that effective C4ISR cannot be accomplished solely by technology, the fact remains that the concept is highly dependent on technical advancements and capabilities. It is imperative to maintain a technological edge over the adversary, in terms of flexibility, innovativeness and redundancy.

Organisational Challenges

Thinking beyond the network. When one talks about C4ISR, it is easier to think about the network that facilitates connectivity rather than the networking. Changing the mindset from thinking about the network as an element of Information and Communication Technology to considering it as a multiple-source composite grouping that needs to be designed and operated in an integrated fashion, is a challenge. If C4ISR development focuses only on technology without system organisational changes, the true benefits may not accrue to the military force.

Qualified Manpower. The optimal utilisation and maintenance of C4ISR systems requires technically qualified and trained manpower at all levels. The human resource needs to be adequately trained and sensitised to operate in relatively flatter hierarchal structure engendered by time-critical demands of modern C4ISR systems. Consequently, they need to handle increased authority and responsibility without looking for higher direction. On the other hand, senior levels of command need to operate at higher organisational and cognitive levels, and allow the tactical Commander to operate independently.

Over-reliance on networks. As C4ISR operations become increasingly complex, the operators become more dependent on technology for maintaining operational efficiency, to sometimes, total exclusion of manual/ semi-automated processes. As a result, valuable conventional means and techniques of data collation and analysis – which may have to be resorted to in the event of major network breakdown / failure – are being progressively forgotten. Therefore, the force needs to identify and maintain old procedures, in order to build adequate redundancies for these networks, and include these in training exercises.

- **Excessive centralisation and micro-management**. As technology matures and large amounts of real time 'tactical' information becomes available to the higher Commanders, They tend to get pulled towards purely tactical decisions; and start interfering with or bypassing the subordinate tactical leaders. Repetitive interventions of this type could render the subordinates either unwilling or unable to take the required initiative commensurate to the developing tactical situation. It is posited that even superior combat power and potential can be considerably compromised by excessive centralisation of C2 and micro-management.

Functional Challenges

- **Information Overload at Higher Command Level**. As data flows from the tactical battlefield to the strategic levels of command, it leads to information overload. The resultant glut of rapidly flowing data could leave the Commander quite overwhelmed to the point where his operational vision may be obscured, clarity of thought may get clouded and decision-making ability could be compromised. Therefore, it is necessary to filter the data with an aim to provide only the most relevant and 'actionable information' to the Commander.

- **Information Overload at Tactical Levels**. The reverse is equally true, if data is passed to the subordinate Commanders without adequate processing. Since his domain of action is quite limited, he needs to receive the most actionable information on priority, to the relative exclusion of other usable assessments.

- **Inadequacy of decision-making tools**. The decision support systems (DSS) are essential statistically enabled tools to analyse vast number of inputs and to make sense of the dynamically changing operational situation. While modern Artificial Intelligence (AI) systems based on Neural Networks have shown promise in decision support mechanisms, it would still be prudent to choose those which provide consistent output of required quality suitable to the peculiarities of the Indian maritime domain. It is also necessary to determine an appropriate balance between automated and manual decision-making processes, to arrive at the best possible mix.

- **Determining the Optimal Mode of Operation**. C4ISR systems are complex systems of systems, and their fool-proof optimal performance cannot always be ensured because of interplay between a large number of constituent elements. Any change in backend parameters like network speed, bandwidth and connectivity, may affect the system adversely. Therefore ensuring optimal mode of uninterrupted operation of critical C4ISR systems must remain the top priority for a Force.

- **Difficulties in holistic testing**. The success of C4ISR efforts depends on complex networks that integrate the elements of various data grids within the Indian Navy as

also those of other armed forces and national agencies concerned with domain related data generation. Since so many organisations are involved, it would be natural to face difficulties during system integration and testing, as the various organisations' subsystems could be operating at different parameters. The ultimate challenge therefore would be to test the integrated national C4ISRsystem as a whole.

Cultural Challenge

- **Resistance to Change**. The most important challenge to adoption of modern C4ISR structure based on net-centric backboneis the cultural resistance from within the organization/s. Adopting the concept of networked centricity requires significant changes in the thought-process of leaders and men alike about war fighting. It may require substantial restructuring of military organisations and review of doctrinal procedures to engage the adversary as a 'joint and integrated entity'. The existence of established and time-tested operational procedures does engender the tendency of the human resource to resist change. Therefore, any change can only be brought about in a gradual and controlled manner, when the benefits of change are recognized, appreciated and imbibed.

Procedural challenge

- **Interoperability**. C4ISR systems envisage seamless connectivity and information exchange between platforms and systems. In addition to the general requirement of inducting interoperable systems, the specific requirements during joint operations with other Forces and during combined operations with forces of different nationalities,

need to be catered for. This can be achieved by the adoption of open standards and interface protocols, which needs to be implemented in a progressive manner.

Way Forward to Meet C4ISR Requirements for Futuristic Warfare

Emerging Command and Control systems will be valuable assets for managing the entire battle space with emphasis shifting from platform centric operations to network centric operations. Cooperative engagement capabilities will seek to exploit the range advantage provided by modern weapons and networked sensors, which may be decoupled from the weapons platform. 'Network Centric Operations' is emerging as a tremendous force multiplier, which will enable availability of all relevant information in near real- time to decision makers permitting substantial compression of timelines for decision making.[6]

The architecture of new generation Command and Control (C2) Systems will need to be modular and scalable with adequate built-in redundancies. They will need to be integrated with other ISR equipment with varying interface protocols. Their architecture should hence, support 'plug and play' features for ease of integration. The software will need to include expert algorithms with AI and auto-learning features to support fast decision-making, and for adapting to the dynamic scenarios. the application software should also be subsequently upgradable to incorporate 'Cooperative Engagement Capability' as the Indian naval C4ISR systems transit from platform-centric to network-centric operations.

The Indian Navy's aspirations to become a truly blue-water Navy in coming years can only be realized if naval commanders at sea are able to synchronise and integrate their high-intensity operations across the world through a network of efficient communication systems. This would require secure global end-to-end information exchange mechanisms

among the units as a critical mission capability; and would also serve as a force multiplier for worldwide readiness, mobility and responsiveness. The most important requirement of naval communications is ship-to-shore and extended-range (beyond line of sight) ship-to-ship communications.

The extended ranges and prolonged duration of ship deployments create unique challenges and complexities. These need to be met by satellite communications (SATCOM) resources. Communication systems designed to support voice, data and video exchanges– including video conferencing– will place High demands on the communication network and large bandwidth. This trend will only grow, leading to a point where earmarking a dedicated channel for each communication task will become increasingly untenable.

Advances in C4ISR have been primarily driven by the commercial sector through tremendous improvements in ICT. Communications technology has already progressed from wire lines to al- digital and optical-fiber or digital microwave. Networks are now electronically switched; and Communications applications and related termination equipment now form a virtual continuum spanning voice telephony, data, imagery and live video. In such a fast-paced technological environment, the Indian Navy needs to pursue the following areas of communications Development for ensuring effective C4ISR:

- **SATCOM PCS**. Fully indigenised SATCOM Personal Communication System (PCS) enabled with capability to exchange voice, video and high speed data links worldwide needs to be realised. This will require a constellation of satellites which could be developed and placed in orbit through coordinated efforts of the Defence Space Agency and ISRO.

- **Security Overlay and Interoperability**. As part of development of Joint Services Interoperable Waveforms for

tri-service interoperability, DRDO has been nominated as the development agency for the waveforms which will be ported over the software defined radios (SDRs).

- **Electronic Warfare**. The indigenous design and development model has worked well for the Indian Navy. Since sufficient expertise about one of the most capable EW systems worldwide, now resides with the developmental agency, the Defence Electronics Research Laboratory (DLRL) and production partner, Bharat Electronics Limited (BEL)); an Advanced Integrated EW system incorporating future technologies needs to be progressed to meet the future challenges.

Intelligence, Surveillance and Reconnaissance mechanisms and systems must be able to provide timely, credible and usable input to enable naval forces to out-think and out-manoeuvre the opposing forces. However, the information gathered is also required to be disseminated to the relevant units at sea in near-real time and in a format, which can be readily utilized for action. This would require high speed modems and reliable, high-bandwidth communication backbone.

A C4ISR system is, in effect, a network of systems at platform level with linkages to the outer world through tactical data links. The technology now exists to integrate all such platforms by a high speed, high bandwidth network so that the firepower of all netted units can be effectively utilised. Towards this, important technologies that need to be developed for Network Centric Warfare include tactical data links, and higher capacity algorithms for Command & Control systems that would facilitate decision-making.

The key to Co-operative Engagement Capability (CEC) is the development of a Common Operating Picture (COP) and distributing the same along and across the entire command and control chain – right

down to the unit level. The concept of CEC is particularly relevant during a theatre-level operation or during a joint missions like amphibious operations. CEC comprises hardware and software that enables real-time distribution and fusion of weapons and sensor data so that individual units can also act as a unified force. The main advantage would be greater reaction time for forces as there would be an early detection of targets. However, robust communication systems with high bandwidths, resistant to electronic countermeasures with a highly accurate positioning system would be the prime requirement of CEC.

A common weapon grid can increase the combat power of the Force by exploiting the capability of high-speed automated weapon-target pairing algorithms. These algorithms can rapidly determine near-optimal weapon-target pairings after taking into account the quantum of threat and resources available–such as number of targets left, remaining rounds, and the probability of kill using remaining rounds.

The command & control systems, tactical data links, associated communication systems, algorithms used for data fusion and data presentation must be standardized and inter operable. this is a major challenge, as it requires that the currently modern systems be downward compatible with existing (legacy) systems; and should be upward compatible with future acquisitions. It is therefore essential that the requirement of interoperability is duly considered while inducting newC4ISR systems.

Protection of C4ISR and NCO systems against deliberate, inadvertent, unauthorised acquisition, disclosure, manipulation, loss or modification of sensitive information has to be ensured through development of secure firewalls. Capabilities such as automatic network intrusion detection and response also need to be developed. The data encryption techniques like key distribution and management by public/private cryp to systems also assumes greater salience. There should also be a provision for

dynamic allocation of network resources to enable continuous operation even in a degraded environment – by isolating the affected system– in case of local breach of network security.

A full-fledged disaster management system needs to be developed so that valuable data generated over a period is not lost due to intentional/ unintentional disaster. Suitable redundancies for data storage and recovery systems locally or in remote locations need to be created for uninterrupted systems operation.

Conclusion

Effective Command and Control is an essential ingredient for conduct of naval operations, both in peace and in war. With improvements in surveillance capabilities, communications, weapon application and networking technologies, timely availability of all relevant information for conduct of naval operations is no longer a constraint. In the existing net-enabled warfare scenario, it is difficult to quantify the benefits of C4ISR, as they are not sequential or singular. Rather, the results are an aggregation of lesser individual factors, adding up to significantly improved effectiveness of overall operational advantage over the adversary in warfare.

The Indian Navy has achieved a lot in adapting to the modern C4ISR requirements in the maritime domain which directly impacts upon India's national security. The geopolitical nature of India's neighbourhood– wherein certain countries either by themselves or in collusion could threaten the national interests of India –increase the demand on the Indian C4ISR architecture. There would always be many challenges in ensuring that the Country's maritime C4ISR network meets the requirement of national security and enable the Indian Navy fleets to erect an appropriate response. However, national security can not be compromised for want of hardware wherewithal or insurmountable challenges.

India has for historically paid a heavy price on account of for its proverbial 'sea-blindness'[7]. The national endeavour should be to ensure that this sordid chapter of history never repeats itself by comprehensive adoption of robust C4ISR concepts, acquisition of capable C4ISR systems and hardware, and integrating them with the national and other services' C4ISRarchitectures in the Navy's operational preparedness matrix.

***Captain (IN) Kamlesh K Agnihotri (Retd)** is a Senior Fellow at the National Maritime Foundation, New Delhi. He was earlier a Senior Fellow at the Centre for Joint Warfare Studies (CENJOWS), New Delhi

Endnotes

1. The IDA cycle is an evolution of the OODA loop (Observe, Orient, Decide, Act) loop. The OODA loop was devised at the tactical level, in relation to air combat. The IDA cycle covers the larger ambit of modern operations at all levels.
2. IHQ MOD (Navy), 'The Indian Maritime Doctrine (INBR 8) -2009,' p. 73.
3. Indian Maritime Doctrine 2009 ibid, pp. 65-68.
4. Parliament of India: Lok Sabha, Unstarred Question No. 4818, answered on 24 March 2021, http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=23710&lsno=17 accessed 01 August 2022
5. Indian Navy, "Information Fusion Centre- Indian Ocean Region", https://www.indiannavy.nic.in/ifc-ior/about-us.html (accessed 03 August 2022)
6. Indian Navy, 2020, 'Swavlamban: Ship's Systems, Weapons, Aviation and Electronics Atmanirbharta Abhiyan' (New Delhi, Naval Headquarters,), p.9.
7. Admiral Arun Prakash, 'China has become a maritime power: It's time India caught up,' Indian Express, 21 June 2021, https://indianexpress. com/article/opinion/columns/india-china-rivalry-maritime-power-navy-7367947/ (accessed 01 August 2022)

171-183

UTILIZATION OF SYNTHETIC ENVIRONMENT FOR DEFENCE EXPERIMENTATION IN PLANNING, EVALUATION AND ACQUISITION OF C4ISR SYSTEMS

Mr Manoj Tyagi et al.*

Abstract

Response to contemporary threats require defence forces to strategize its war fighting capabilities through adapting newer command and control structures, planning for sensors, weapons and communication systems. There is a need to quickly assess the aptness of a selected capability against the threat, through Operational Analyses (OA) tools and techniques. The measure of effectiveness and merits are to be arrived to prove a hypothesis of success of such concepts, systems, in a particular threat-scenario.

A readily configurable framework to test and prove the conceptual manifestations is need of the hour. A contemporary approach to capability development is required-one that uses experimentation, rapid concept exploration, and prototyping to integrate materiel and non-materiel solutions in ways that most effectively address war-fighter capability gaps. This paper proposes such a framework which maximizes effectiveness through continuous and iterative experimentation to bring alignment, rigour, efficiency and faster insertion of new capability. This ecosystem aims to provision analytics-based development, tactical planning and acquisitions in Command, Control, Communications,

Computers, Intelligence, Security, and Reconnaissance (C4ISR) systems.

Introduction

"*Anything we use today arrives through a process of organized experimentation; over time, improved tools, new processes, and alternative technologies all have arisen because they have been worked out in various structured ways*".[1]

Lack of such an approach can lead to undesired consequences [2]. On the contrary, utilization of the approach can be advantageous [3].

Modelling and simulation is the technique of representing and virtually executing complex systems, processes, system of systems. A 'System of Systems (SoS)' is a concept where various heterogeneous systems become participants in a scenario and the conduct of scenario itself is treated like a system. Essentially, SOS is made up of components, which are systems, interactions & events, processes & activities, resources, assumptions & constraints and operating environment. The aim of such a representation and virtual execution can be to educate / train people on skill, tactics, decision making, or to analyse various typical-to-futuristic scenarios. To enable smooth design, development and execution of such a training or analysis exercises requires an infrastructure, referred to as Synthetic Environment (SE).

SE includes computing hardware, networks, software tools, models, simulations, people, and real equipments like sensors, weapons, or platforms; to form a common representation of a realistic typical / futuristic scenario in virtual or synthetic world. SE is typically used for simulating a wide range of highly interactive activities, including the human, to enable generation of 'enough data' for the purpose of analysis. SE can also be utilised for research, training and evaluation. Figure 1 shows the purpose of models, simulations and synthetic environment.

Figure 1: Purpose of Combat Models

The proposed facility would be basically a synthetic environment (SE), and will be exploited for operational analysis (OA) using defence experimentation (DE) approach. “Defence experimentation is the application of the experimental method to the solution of complex defense capability development problems, potentially across the full spectrum of conflict types, such as war-fighting, peace-enforcement, humanitarian relief and peace-keeping” [4].

Operational Analyses (OA)[5]

Operational Analysis (OA) is concerned with the study of complex decision-making problem often characterised by incomplete and uncertain information on various aspects of problem space. Typical decision-making problems involve the allocation of scarce resources

in the systems where effectiveness is measured against an array of multiple, and usually conflicting, objectives. Following is a listing of typical OA scopes for defence industry analysis:-

- Force Structuring
- Military task evaluation
- Capability gap analysis
- New capability Requirements
- RFP / RFI / Requirement document generation support
- Logistics / Through life
- Cost Effectiveness
- Campaign planning and mission rehearsal / training
- Operational support
- Doctrine / Concept proving and development

The OA process through defence experimentation brings together the assumptions, options, data and expert judgement relevant to the operation of a particular system in a particular context and examines their implications in a structured, explicit and auditable way using models and simulations. As a first step, OA approach identifies the alternatives between which a decision is to be made. Secondly, the criteria against which these alternatives are to be judged are defined (measure of performance and effectiveness). Thereafter, a synthetic environment is configured to carry out defence experiments, to generate 'enough' data for statistical insights and analysis.

Capitalization of commercial information technologies for C4ISR systems are proving a game changer and essential step for development of interoperable and flexible systems to support joint operations

and leveraging of inter service military assets. Similar approach for commercially viable ecosystem for Advanced Modelling & Simulation and Experimentation (AMSE) is necessary for viable and effective Operational analysis (OA) using defence experimentation.

Defence Experimentation

In general terms, experimentation answers the question, “If I do this, what will happen?” *Defense experimentation*[6] extends that question to the military domain, providing decision makers with information they need to make good decisions. Defense experiments provide opportunities for technologists and warfighters to evaluate potential solutions to existing or emerging warfighter capability gaps and probe the integration of technology development and concept exploration in order to maximize synergies that exist. Experimentation also enables rapid evaluation of a military problem, increasing the speed by which knowledge and understanding is gained and decisions can be made. Experimentation fuels the discovery and creation of knowledge and leads to the development and improvement of products, processes, systems, and organizations.

Development of Tactics, Techniques, and Procedures (TTP); development of CON-OPS, Planning and Rehearsal of complex missions and Joint Operations, Simulation Based Acquisition (SBA); Course of Action Development and Analysis; and Execution Monitoring are some of the challenges in development of C4ISR systems that can be addressed through analytics-based Defence experimentation.

Necessity of commercial Synthetic Environment (SE) ecosystem

An Advance M&S and Experimentation facility requires state-of-the-art modelling & simulation and analysis suits and excellent 2D / 3D visualisation software. It requires high-end presentation facilities for

internal as well as strategic decision makers, including well designed conference, exercise control and experimentation area / labs. Typical tool suit available in such a facility are: Terrain Visualization Tools, Platform/Weapon/Sensor Models (Virtual as well as Simulation), 3D Model Development Tools, Aggregated Force Models, Civilian

Figure 2: Synthetic Environment

Behaviour Models, Sensor detection, identification and tracking models and Communication Models as pictorially depicted as in Figure 2.

Defence Experimentation (DE) through Synthetic Environments (SE) is the key to success in maintaining lead in defence markets in India and abroad. It's all about how fast and credibly we can predict and satisfy our customers' needs. Inherent concepts for defence experimentation are:

- Capability gap analysis
- Technology planning
- Military requirement analysis
- Verify concept of operations (CONOPS): Experiment

before building system/sub-system to arrive for “optimal” specifications / intended operational purpose

- Test the system deployment, virtually, for “best-plan” in an operational environment

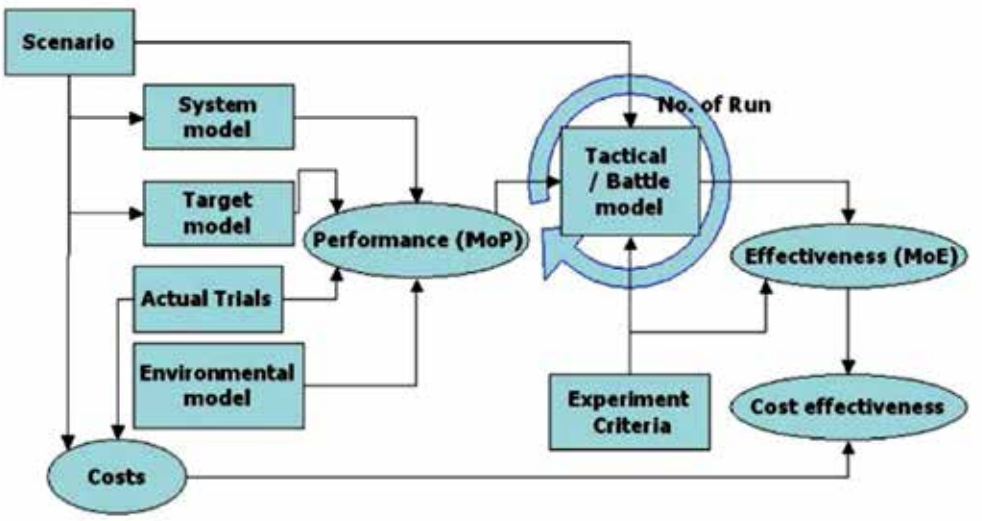


Figure 3: OA through DE framework

- Cost effectiveness studies
- Evaluation and What if analysis.

Lets us consider an exemplary framework given in Figure 3, for operational analysis of a system. Such a framework provisions, tools and processes to carry out studies as listed in ‘Inherent concepts for defence experimentation’ above. Clearly, it would be required to iteratively change experiment criteria and re-configure models and simulation. User participation is a must in such experiments. The scenario executions (scenario stage through to obtaining measures of effectiveness) often involve user inputs and user decisions in the tactical battle area. We also

require subject matter experts (SMEs) to validate fitness for purpose of models and simulations.

Benefits of Defence Experimentation (DE)

Defence experimentation provides important insights and understanding of the operation of the system. It leads to quantification of the comparative performance of the systems operating under different conditions. Finally, Operational Analysis (OA) using Defence Experimentation (DE) becomes a more objective and justifiable basis for management decisions on the operation of the system. Other advantages as compared with other alternative like field trials, development of and thereafter experimentation on prototypes and live exercises like war games are[5]:

- Cost effectiveness
- Time can be compressed
- Control is easier
- Safety is not a problem
- Applicability is very wide
- Visualisation aids understanding

However, care must be taken to define 'achievable goal' and ample level of 'actual' user participation must be ensured for defence experimentation. Additionally, the model / simulations used in the SE should be verified / validated by subject matter experts (SME).

Experiment Development Process

Experiment process starts with seeking and establishing a hypothesis like, "If Air Command and Control System is to be inducted by Defence Forces[7], then they would be better in terms of identifying and neutralizing threats". What is actually meant by "better", can be defined in measures

to be captured or derived during and after experiment runs. Experiment Development Life Cycle (EDLC) can at least be divided into two logical parts, Development & Usage. Development part phases and activities require technical expertise in modelling & simulation and software design & development. Engineer is expected to learn, configure, script, program, interface, interoperate[8] and manage bespoke & COTS software. Usage part phases and activities require expert level knowledge of conduct of wargames and operational analysis to conduct of experiment runs, collect relevant data, quantify, analyse in details all measurements and portray consolidated results supporting or rejecting the hypothesis.

Following are concise activities under experiment phases:

- Preliminary: Identify experimentation opportunity and develop concepts.
- Problem Formulation: Formulate crisp problem & proposed solutions
- Experiment Design: Design scenarios, define MOPs / MOEs, plan experiment, technical and participants, generate event and feature list for proposed solutions.
- Experiment Development-Capability: Develop required features, solve issues, conduct trials, refining scenarios, and training.
- Experiment Execution: Conduct, control, monitor and log runs
- Analysis: Consolidate results, derive and analysis measures.
- Report: Producing conduct and run reports, analysis on MOE report.

Defence Experimentation Case[9]

The Command, Control, Communications, Computers and Intelligence (C4I) Systems provide situational awareness about operational

environment and supported in decision making and directed to operative environment. These systems had been used by various agencies like defense, police, investigation, road, rail, airports, oil and gas related department. The increased use of C4I system had made it more important and attractive. Consequently effectiveness of such systems needs to be established.

A scenario encompassing major aspects of C4I system is formulated. Objective from utilization of C4I system in this scenario is defined, e.g. “Monitor, identify and neutralize threats”. Measurable parameters to indicate effectiveness of C4I system in the scenario are listed. Parameters in this scenario can be: threats in the scenario, threats identified confirmation to threats neutralization, time to react, damage to own resources etc.

The scenario is executed and values of various parameters are noted.

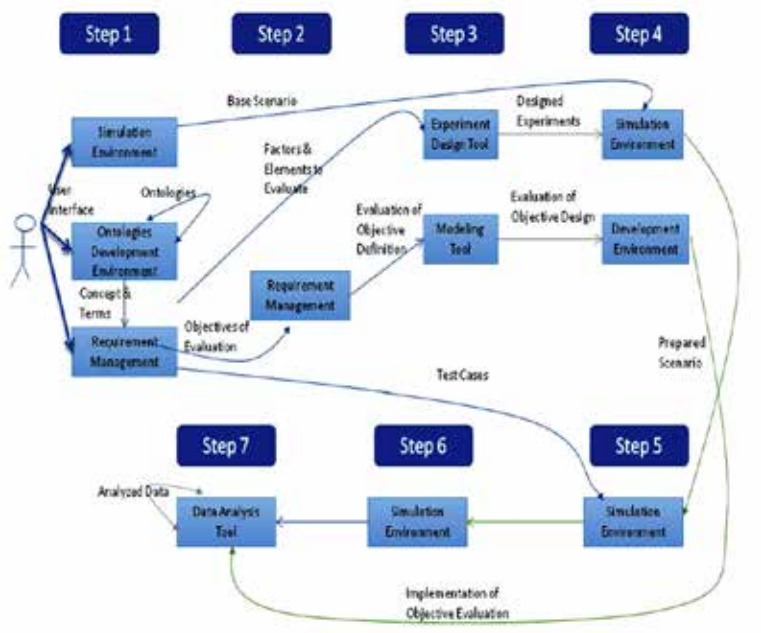


Figure 4: Methodology

Methodology

As shown in Figure 4, Using *Synthetic Environment* as a Tool, *Defence Experimentation* Method is applied in a scenario to describe Hypothesis (e.g. *Force Multiplier Effect of C4I systems)*.

It shows variety of external environment requirements that can act as input to Simulation Environment, thus moving closer to the real external environment. Combination of some real inputs with Simulation tools can result in another Simulation Environment. Development Environment, which represents inner capabilities, is catering to variety of capability requirements and can be changed by adding / removing / editing capabilities.

The plan is to baseline the measured parameters, by having some “as it is” runs, and then one by one introducing capabilities and observing the effect in measured parameters across multiple runs (four to five runs per capability). Graphs to show the different stage outputs of the data are collected, analysed and presented in form of bar charts and increase / decrease of measured values in percentage when a capability is introduced and what can be said about its hypothesis. Data would also indicate if more number of runs is required. Also, comparison of various capabilities can be derived from the data output.

Thus, from outputs analysis, capabilities (e.g. of C4I systems/sub-systems) conforming to hypothesis can be added and others can be removed.

The decision maker now has the understanding of the scenario and data support for decision making. Important point to note here is that these capabilities may be at production state or at design or even conceptual level for the company. The requirement for defence experimentation is that only equipment’s / capabilities’ basic characteristics/ features should be known, for proving / supporting a hypothesis. This brings out that

the field of defence experimentation can be utilized at various stages of product/capability development cycle.

Conclusion

Constitution of Centre of excellence for Defence Experimentation using Synthetic Environment is need of the hour. Such a rapidly configurable CONOPS experimentation laboratory has credible potential to be utilized across joint defence programmes to:-

- Reduce time of prototyping / concept proving and supporting
- Moving beyond measures of performance, to measures of effectiveness/merits for quantifying force-multiplier effect of produced equipments.
- Increase cost-effectiveness by reducing field trials

The facility and method described in the paper would prove to be a contemporary approach to capability development — one that uses experimentation, rapid concept exploration, and prototyping to integrate materiel and non-materiel solutions in ways that most effectively address war-fighter capability gaps.

*__Mr Manoj Tyagi__, currently working as DGM, Network Centric Systems, Bharat Electronics Ltd, Ghaziabad has done Masters in DSM (RMCS, Cranfield University, UK) and is a former Scientist at Institute of Systems Studies and Analyses, DRDO

Co-authors:

Mr Varun Gupta, Manager, Bharat Electronics Ltd, Ghaziabad

Mr Sandeep Kumar, Manager, Bharat Electronics Ltd, Ghaziabad

Mr Amit Gupta, Sr DGM, Bharat Electronics Ltd, Ghaziabad

Endnotes:

1. Thomke Stephan H., “Experimentation Matters; Unlocking the Potential of New Technologies for Innovation”, Boston: Harvard Business School Press, 2003, p. 307
2. Seth G. Jones, “Russia’s Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare”, CSIS Briefs, https://www.csis.org/analysis/russias-ill-fated-invasion- ukraine-lessons-modern-warfare, June 1, 2022
3. Ralph D. Thiele, “Over five years of Russian hybrid warfare against Ukraine provide lessons how to make Ukraine stronger”, ISPDW Strategy Series: Focus on Defense and International Security, https://www.ispsw.com/wp-content/ uploads/2020/01/662_Thiele.pdf, Issue No 662, January 2020
4. “Understanding and Implementing Defense Experimentation (GUIDEx)”, NAMRAD- TTCP-JSA WF Experimentation Group,Version 1.1,March 2006
5. Searle, Jonathan R. (Manager SSEL), “Course notes and Handouts for Networked & Distributed Simulation module of MSc course in DSM”, ESD- RMCS, Cranfield University, April 2005
6. “Department of Defense Experimentation Guidebook”, https://www.dau.edu/tools/Lists/DAUTools/Attachments/381/DoD%20Experimentation%20Guidebook%20 v2.0%202021.pdf, Nov 18, 2021, p. 2
7. Karyn Matthews, Mike Davies, John Dunn, Carsten Gabrisch (1997), “Synthetic Environments for C3I Experimentation”, Information Technology Division, Defence Science and Technology Division, Salisbury
8. LTC Robert L. Bethea (Jr. U.S. Army) (2003), “Joint C4I Interoperability– A Look At The Process For Army Transformation”, USAWC Strategy Research Project, https://apps.dtic.mil/sti/pdfs/ADA414829.pdf
9. Michael R. Hieb, Lieutenant Colonel Donald H. Timian (1999), “Using Army Force-on- Force Simulations to Stimulate C4I Systems for Testing and Experimentation”, https://apps.dtic.mil/sti/pdfs/ADA461500.pdf

STANDARDISATION AND CODIFICATION A PERSPECTIVE FOR DEFENCE FORCES AND INDUSTRY

Cmde Gopal R Wani, Director, Directorate of Standardisation- MoD/DDP*

'**Those who don't learn history are doomed to repeat it'**, this quote from philosopher George Santayana highlights the importance of the lessons that we must derive from the events that occurred in the past. Standardisation is one such process that the world came to understand and adopt when the Allied forces in the WWII could not get the war equipment of interchangeable nature. This in turn resulted in the formation of International Organisation for Standardisation (ISO) which defines standardisation as under:-

"The process of formulating and applying rules for an orderly approach to the specific activity for the benefit and with the cooperation of all concerned and in particular for the promotion of optimum overall economy, taking due consideration to account of functional conditions and safety requirements"

From both logistics and economic considerations, lesser the variety of items purchased, stocked, transported and used by the services, the better the war preparedness and fighting fitness. In India, the benefits of Standardisation were realised as early as in 1959 when Standardisation Committee was set up under the Hon'ble Raksha Mantri and based on the recommendations of the committee, Directorate of Standardisation

was set up in 1962 under a full time Director under the administrative control of Department of Defence Production & Supplies.

Standardization supports the achievement of commonality and interoperability in Defence Services. It is the enabling tool which provides Defence Forces with systems that are interoperable, reliable, sustainable and affordable. Standardisation is also an essential tool of Logistics Management in Armed Forces. Lesser the number of items procured, stocked, transported, maintained and used by troops in the field, the better it is for efficient management. The main aim of Standardisation in Defence is to optimise the existing inventory without affecting the preparedness/ efficiency of the Defence Forces. A standard is a document that establishes uniform engineering or technical specifications, criteria, methods, processes or practices.

Directorate of Standardisation is responsible for ensuring standardization and codification activities in all fields in the Ministry of Defence under the control of Department of Defence Production within the broad policies formulated by Standardisation Committee with following objectives:-

- Codification of Defence inventory to ensure uniform pattern of numbering the items and denoting each item by a well defined scientific nomenclature.
- Variety Reduction through preparation of Standardisation documents like Joint Services Preferred Range(JSPR) and Joint Services Rationalised List (JSRL).
- Entry control to check proliferation of Defence inventory.
- Preparation and promulgation of Joint Service Specification (JSS), Joint Services Guide (JSG) and Approval Notification (AN) for reference and use by defence services.
- Assist in formulation of Joint Services Policy Statement (JSPS) and Joint Service Qualitative Requirement (JSQR)

for procurement of products by services.

- To be repository of Indian and Foreign Standards for the use of Defence Services.
- To facilitate IT enabled services for accessing Standardisation/ Codification databases, standards and specifications.
- To adopt fast changing technology thereby providing better services.
- To ensure that the standards produced are compatible to IS & International standards.
- To co-ordinate and conduct Standardisation programme at National, Inter Service and Intra Service levels.
- To promote adoption of “SI” units in Ministry of Defence.
- To codify all transactions under the Defence Inventory using NATO Codification System (NCS).
- To maintain a Data Base of codified Defence Inventory for the purpose of Rationalisation, Standardisation, Simplification and ‘Entry Control’.
- To maintain and run Technical Information Centre for all Standardisation activities.
- To print, stock and issue Standardisation Documents, Compendiums and Catalogues for the Ministry of Defence Units.

Standards are to be seen as a lever for upgrading the country’s industrial base. We should focus and strengthen research on standards in new technology fields like AI, Big Data, Block Chain and C4ISR. The idea is to formulate high technical standards essentially forcing manufacturers to upgrade their process and ensure interoperability inter-service and intra-service with all available vintage equipment. This standardisation in new areas of technology areas will provide economic leverage and enhance India’s competitiveness.

INSS

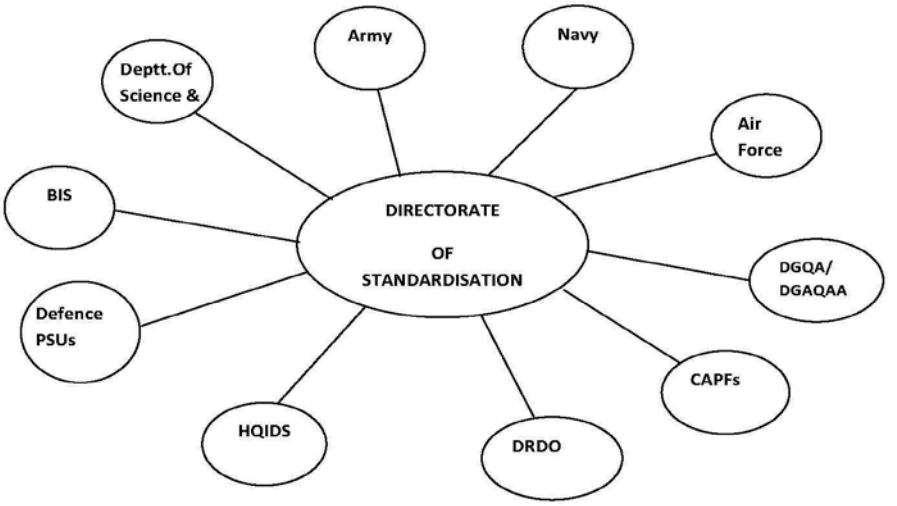
The Indian National Strategy for Standardisation (INSS) framework was released in Jun 2018. INSS provides direction for Indian Political and executive leadership on how best to use standardisation, technical regulations, quality infrastructure and related activities to advance the interests and well being of Indians in a global economy. This framework will provide far reaching benefits to economy and will raise the credibility of "Make in India" brand in global market. It will help align the strategy of sectors with national priorities and policies. This will also leverage the best practices and innovations from across the globe and ensure a facilitating environment for next leap of transformation. The Four pillars of INSS are:-

- Standards Development
- Conformity Assessment, Accredition and Metrology
- Technical regulations and SPS measures
- Awareness, Counselling, Training and education

As part of INSS efforts DoS has been accredited as "**Standards Development Organisation**" **(SDO)**. The standards developed by DoS will be recognized as National Standards. Recently DoS has initiated few Standards for items having Dual use (Civil & Military) for acceptance as National Standards. Directorate of Standardisation interface with the various organisations (including CAPFs) as shown below to establish effective standardization activities and hormonisation of standards within the services:-

Codification of Item of Supply

Codification is the process of standardizing and developing a norm for a common identification language. Directorate of Standardisation is a member of Allied Committee (AC/135) the Apex Body of NATO Codification System (NCS). This has placed Indian Codification System



at International level and DoS has attained the status of being National Codification Bureau (NCB).

Codification of any item of supply is considered as a mandatory activity to identify the item with a unique number which provides the detailed information of the item/product alongwith the details of manufacturer. To achieve the internationally adopted codification pattern, Directorate of Standardisation also designated as National Codification Bureau(NCB) of India has adopted the NATO Codification System (NCS) towards codification of item of supplies by allocating NATO Stock Number (NSN) to each item and unique NCAGE code to each manufacturer since 2016 and has achieved the Tier-II membership status in NCS. Prior adopting NCS the codification of defence inventory was being undertaken using in house codification software CODISAP to generate the DCAN Numbers. However, to align with International community and ensuring uniform codification pattern for all item of supplies ex-import from NATO nations and members of Allied Committee/135 the NCS has offered an edge to Indian Codification System.

Benefits of Codification

Today, more than sixty countries around the world use the NCS in some manner within their logistics systems. Most of these countries assign and use NATO Stock Numbers (NSNs) as a key to logistics data. NATO Codification offers many significant advantages to countries participating in the NCS, as well as to NATO organizations and private sector participants outside the Defence community.

The NCS is often referred to as an international language of logistics. It is not an inventory control system; it is the logistics language used by such systems. Likewise, it is not a supply accounting system, but the logistics language used by supply systems, procurement systems, maintenance systems, storage and distribution system, disposal system and transportation systems. The NCS is the foundation of inter-service and inter-country logistics cooperation. The NCS provides a common supply language in NATO and supports multinational logistics operations in countries that have treaties with the United States to participate in assigning and using NSNs.

Essentially the NCS is used for two purposes:-

- To save money
- To aid logistics operations

Save Money

***Inventory Reduction*.** Logistics managers need to know where stock is located and how much is available. If the NCS is used (as part of an inventory control system) they have a tool to identify interchangeable items in different locations nationally or internationally. Thus,it prevents buying unnecessary stock, avoid storage costs for overstocked items, and use items before they become out of date. By using standard methods for identifying and tracking items two private companies

reduced inventory by $75 million and $97 million respectively by using tools like the NCS.

Avoid New Inventory. Since equipment often has common parts with other existing equipment, the NCS can be used to eliminate duplicate items in the supply system. In the United States, a large producing country, they have experienced that parts for brand new equipment match existing parts in the catalog more than 30% of the time.

Lower Purchase Prices. Various purchasing offices within a nation may buy the same items. If the NCS is used (within a procurement system), senior managers can quickly identify duplicate purchases and compare prices. This allows them to consolidate purchases into larger packages to negotiate lower prices.

Aid Logistics Operations

Cross Service Supply. The NCS aids cross service supply between the military branches (when used within a supply system). Thus, a Navy supply operation can supply a local Air Force contingent since they both use the same method for identifying items of supply. This saves money too, since redundant supply operations are expensive. Again, these savings are even more important at the Alliance level.

Interoperability Between Countries. The NCS being international codification system also facilitates the sharing of supply support between countries. Use of a common language understood by everyone simplifies the technical dialogue between countries and users. For example of this benefit, the NATO experience in Bosnia where peacekeeping force from a non-NATO (and non-NCS using) nation arrived without repair parts. Within a very short period of time, some 30% of their equipment were unserviceable for lack of spares. They were unable to ask for support from other nations because they did not use any relevant materiel identification system. Finally, the French forces used the NCS to help

them identify the spares they required and, eventually, the problem was resolved.

Reduced Equipment Downtime. Military services in the area of operations and logisticians are in a better position to get the right parts to the right place, in time.

Quicker Identification of Supply Items. An accurate description of items, combined with an easy to use catalog, allows supply personnel to more quickly identify needed items.

Better Tracking of Vendors. The NCS includes a system for identifying and tracking commercial vendors. Combined with procurement systems, managers can more systematically track such critical information as past performance by the contractor, addresses and telephone numbers, and political/social data (such as geographical distribution of vendors and manufacturers within a country and minority group ownership).

History of Commercial Sources. Logisticians can use the NCS to determine past sources for purchases of the item of supply. This can be useful when items are difficult to obtain.

Aid Domestic Industrial Base. When a company's reference number is recorded on an item of supply in the NATO Master Catalogue of Reference for Logisticians (NMCRL), it is visible to other countries as a potential source for that item. Thus, the company's opportunity for sales is improved.

What is NSN?

The NSN was designed to be usable by both humans and machines. Without exception, NSNs are numbers that are thirteen digits long. The first four digits classify items into logical groupings. The remaining nine digits make each NSN unique. The most important advantage of NSN is that almost everyone in government and business, worldwide,

recognizes and can use it. This is true for computerized systems as well as human management of supplies because the format of NSNs is always consistent.

The process of assigning and maintaining NSNs is a collection of activities called cataloging. When a new item is ordered often enough, or when a new weapons system enters service, cataloging activities are initiated. A wide range of logistics data is assembled about that item including price, item name, manufacturers part number, physical characteristics and many other kinds of data. This data collection process is the backbone of cataloging. The system then assigns the next available number and a new NSN is created. All of the data about an item of supply is referenced to an NSN and an item of supply manufactured by many manufacturers, if it has the same form, fit and function, it is assigned only one NSN. As the central link between all of the various kinds of logistics data it allows efficient, reliable management of logistics data, and of the items themselves. Without NSNs, management would be difficult and confusing because the NSN is the key that unlocks the rest of the data.

Benefits of NSNs – Cost Control and Exact Identification

Cataloging, and its use of NSNs, supports logistics managers with a standard method of identifying and tracking items. Managers can rely on the structure and attributes of items cataloged by NSN to avoid purchase and storage of unnecessary stock, and to use items before their shelf life expires. Supply managers use the classification inherent in the first four digits to group similar items for improved management. Use of NSNs also helps managers avoid purchase of duplicate inventory, account for existing inventory, and negotiate lower purchase prices for new inventory by reviewing pricing information.

NSNs play a central theme in the emerging role of contractors supporting

military operations as well as in the continuing integration of the Services in joint military maneuvers. An item may be purchased from a contractor, delivered by the Air Force, distributed by the Navy and used by the Army. The importance of using a single language of supply, such as the NSN provides, becomes increasingly important.

The manufacturer of any item of supply on request can be allotted a unique internationally recognized Manufacturer registration code i.e., NCAGE (NATO Commercial and Government Entity) code which is mapped to the NSN of the item of supply. Therefore, visibility of the manufacturer through NCAGE code for the respective products when visible to the nations using NCS would yield ample opportunities for the national defence product manufacturers to enhance the export potential and lead the nation towards AATMANIRBHARTA.

Our Commitment

Directorate of Standardisation, MoD/ DDP as National Codification Bureau(NCB) of India plays an important role in implementing standardization within services and supply management by issuing and managing the use of NSNs. We are partners with all the individuals, manufacturing units, quality assurance agencies (AHSPs/ Responsible Organisations) and nations who depend on accurate, efficient cataloging to acquire and use millions of items of supply. It is the commitment of NCB, India to lead logistics innovation in NSN management for the benefit of our Services and Indian Industry.

***Cmde Gopal R Wani,** is appointed as Director, Directorate of Standardisation, MoD/ DDP New Delhi.

ADVISORY BOARD & EXECUTIVE COUNCIL
CENJOWS

Printed and published by Lt Gen Sunil Srivastava on behalf of Centre for Joint Warfare Studies (CENJOWS), 301, B-2 Wing, 3rd Floor, Pt Deendayal Antyodaya Bhawan, CGO Complex, Lodhi Road, New Delhi-110003, and printed at M/s. Xtreme Office Aids Pvt Ltd., Plot No.11, Basement, Below Canara Bank, Commercial Complex, Nangal Raya, New Delhi-110046.

Editor: Lt Gen Sunil Srivastava (Retd)