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