DATA: THE NEW MUNITION FOR JOINT WARFARE

Gp Capt Ankur Mathur

Abstract

Sometimes, existing technologies converge, mutate, or get creatively applied on battlefields to create a unique winning concoction. The fusion of big volumes of digital data and its assured transmission through battle networks is a crucial element of the modern battlefield. The side that manages it better, wins. Many emerging military technologies have data management integral to them. At the heart of emerging concepts of Multi-Domain Operations (MDO) is the ability to seamlessly transfer data across various domains. Cross-domain data transmissivity is therefore going to become an important capability, in ruggedized devices and networks. To overcome these, the Indian Armed Forces must implement modern data management concepts based on cloud computing and edge computing. To navigate the digitally connected battlefields, there is a need to formulate a Defence Data Policy framework. For establishing a tri-service data cloud and network protocol of cross-domain connectivity. IAF can be the lead service.

Introduction

Technology has always impacted warfighting. With emerging technologies, new concepts of warfighting emerge. Some of these concepts and their application on the battlefield profoundly impact the outcome of wars. Scholars refer to them as the Revolution in

Military Affairs (RMA). The human History of Warfare is replete with such examples. Whether it was the horse-driven chariots of the Indus Valley, or the Huns, Turks and Mongols who graduated from chariot to horse-riding, or the Chinese gunpowder that enabled a Musketeer to fire bullets from a distance, it was soon realised that when men of equal worth fight on unequal terms, the side with better weapons win[1]. However, it was not always the latest or the most advanced technology of the era that tilted the balance on the battlefield. Sometimes, it was the synthesis of existing technologies, their mutations, their creative application, or their convergence that created a unique winning concoction. A case in point was the success achieved by the 'great ships' of the European mariners of the 16th Century, who successfully combined their ship-building prowess with broadside firing cannons using gunpowder; shipbuilding, cannons and gunpowder being commonly known technologies at that time. Their convergence on a battleship changed the course of the history of naval warfare, and that of European Colonialism.

It is the converging technologies of today that have prompted some scholars to believe that 'The Future is Faster' than we think.[2] Converging technologies have transformed businesses, industries and even our daily routines. A case in point is the smartphone in our pockets which is fast, compact and much more powerful than a decade ago. Technology, in the military, will continue to have a huge impact. However, when it comes to forecasting warfare-based technology, the task becomes complicated. War tests technology to the hilt. War is also the testbed of technology. Hamish McRae, in his book 'The World in 2050' offers his advice on how to think about technology and its impact on the future[3]. As per him, the advancements in technology can be incremental or revolutionary. Incremental advancements, he says, are generally bounded by the Laws of Physics. But when human desires get added, which is what warfare has been all about, then revolutionary changes may also occur. Revolutionary technologies belong to the realm of 'unknown unknowns' and therefore are being left out of the scope of this paper.

The incremental rise in digital data across all facets of humanity and its processing has so far been following 'Moore's Law'[4]. The fusion of big volumes of digital data that gets generated by today's platforms and its assured transmission is one such arena that can potentially tilt the balance of force application towards the side that manages it better.

Data: The new Munition

Information and Communications Technologies (ICT), 5G/6G Wireless Networks, Artificial Intelligence (AI), Big Data Analytics, Machine Learning (ML), Autonomous Unmanned Vehicles, Sensor Fusion, C4ISR grids, and many more such emerging technologies have data management integral to them. In fact, at the heart of emerging concepts of Multi-Domain Operations (MDO), Joint All Domain Command and Control (JADC2) and Advanced Battle Management Systems (ABMS) is the ability to seamlessly transfer data across various domains[5]. Cross-domain data transmissivity is therefore going to become an important factor in any future battlefield.

Data has a crucial role to play in Defence Intelligence and ISR. Large datasets are generated by various ISR platforms, Satellites, the Internet, Social Networks and Digital Communications. For Defence Intelligence Agencies, sifting through this data becomes a challenge. Other hurdles of quality assurance, inter-agency security and legal compliance must be crossed before data can be presented for Command and Control (C2) functions or for the sensor-shooter loop. Of course, data needs to be tagged with a time stamp. Intelligence data in today's Information Age has a limited 'Shelf Life'. Hence, customised and intuitive products at the speed desired by modern wars are possible only through employing techniques of data sciences[6].

Artificial Intelligence (AI) promises to help Defence Intelligence Agencies overcome the '3V Challenge' (volume, variety and velocity) and reduce the risks concerning '2V' (veracity, value).[7] However, we now know how algorithms can be misinterpreted, what is now referred to as artificial stupidity.[8] Algorithms, if revealed to the adversary, can also be exploited. Better algorithms, apart from logic, require bigger data sets. Thus, as AI evolves from stupidity to intelligence, the need for big data is going to be insatiable.

Information Technology is transforming modern Air Defence architectures as well. The requirement of a robust air defence is well known. John Warden once remarked that "since the German attack on Poland in 1939, no country has won the war in the face of enemy air superiority."[9] To deny air superiority to the adversary, all modern air forces have been integrating their air defence elements across domains to achieve an Integrated Air Defence

System (IADS). Modern IADS include air surveillance, weapon control and battle management functions. By integrating various Surface Air Missile (SAM) systems, these IADS follow a 'System of Systems' approach.[10] As a C2 function in Battle Management, they enable seamless passage of data even to the last echelon, thereby improving redundancies, depth of communication and span of control. Multi-domain integration and multi-effect approach with malleable communication are key ingredients of modern IADS.

For an effective 'kill chain', these IADS are increasingly relying on functions like Threat Evaluation and Weapon Allocation (TEWA) to act as a decision assistance tool. Apart from technical data, a large quantity of historic dataset is required to provide the predictive modelling capability to these tools. As air defence threats expand into near-space (20-100 km), the role of these IADS will also expand to include Ballistic Missile Defence (BMD) capability and Space Domain Awareness (SDA) features. Data integration, correlation, distribution and dataset-based decision-making will therefore become quintessential.

All this is only possible if cross-domain data transmission protocols are well established. Data, its storage and analytics, and its transmission through associated battle networks are thus the new munition of warfare, ready to be employed effectively in 'Informationized' warfare. Likewise, its denial to the adversary, and disruption/ destruction of its associated networks, make it a legitimate target throughout the full spectrum of warfare.

Data: In Military Matters

Military Data and its associated ICT devices have certain attributes. Military organizations devote a large chunk of their ICT resources to ensure the secrecy of data. In the contested battlespaces, they also need to ensure that data transmission remains jam-resistant. Use of spread-spectrum techniques along with encryption are used to ensure data security and data assurance to the end user. Along with the digitisation of sensors, processing and decision elements, communication elements are increasingly becoming digitised. For communication links, apart from requirements of resilience to jamming, spoofing, interception and disruption, latency becomes an important factor. The need for near real-time data transfer of communication networks is an important factor in designing communication architecture. High latency makes communication ineffective. A case in point is a high latency of 0.5 seconds achieved by satellite-based communications operating through Geostationary Earth Orbits (GEO).[11]

Ruggedization of ICT devices and associated networks is a prerequisite that all military organizations must cater to. In addition, ICT devices in various domains viz land, sea, air and space, need to have ruggedization features suited to their medium. For example, land-based devices must cater to high temperatures and dust resistance, those at the sea would require saltwater protection while those in the air must cater to high vibrations and temperature variations up to several degrees sub-zero. Space ICT devices requires a special type of hardening, one that caters to a hostile space environment. Thus, unless ruggedized, most commercially off-the-shelf (COTS) ICT devices are unsuitable for military needs.

Military, unlike its civil counterparts, has no choice in deciding its workplace. The 'Work from Home' feature is ruled out. Moreover, their 'offices' vary from icy peaks to remote jungles, thousands of feet above the terra firma to meters deep in the oceans. These 'offices' are also prone to frequent relocation as per the needs of the situation. Their remoteness, and thus lack of a readymade ICT infrastructure leads to low data transfer rates at the end user. Hence, many of the existing ICT solutions, currently employed by Global Businesses and Industry, need tweaking to make them compatible to military use. To overcome the challenge of end point connectivity, militaries across the globe are trying to employ WiFi and SATCOM (Satellite communication) links. Both however have low bandwidth as compared to Optical Fibre Cable (OFC) enabled networks. However, as the incremental technologies progressively evolve, 5G/6G WiFi networks and Low Earth Orbit (LEO) satellite-constellation-enabled StarShield network (military version of Elon Musk's StarLink) are promising high-speed low latency data throughput rates as high as 610 Mbps.[12]

Information Technology (IT) in the 21st Century has continued on its upward trajectory. As storage, networking and data processing speeds improve; this along with the falling manufacturing costs and increased miniaturization of chips are paving the way for new IT products each year. Cloud Computing is one such technology that has shown promising results. With a Cloud, it is possible to back-source the processes of data storage, applications, services, security, management and even infrastructure[13]. Private Enterprises benefit from it as these Cloud services are available for hire, thereby reducing the cost of maintaining and sustaining them. The idea has caught the attention of the Defence Industry as well, with many well-known companies like Thales offering Defence Cloud services for Military use.[14] US Dept of Defence (DoD) has issued detailed guidelines in the form of the DoD Cloud Strategy in 2018 to leverage the technology for US Military.[15] The US Army, in 2020 has come out with its independent document in the form of The Army Cloud Plan.[16]

It therefore seems that Cloud Computing may have all the answers to the challenges of Military data handling. Not quite so. Cloud Computing has solved the problem of data processing and storage by obviating the size, weight and power requirements of the equipment required at the tactical end of the battlefield. However, Cloud strategies rely heavily on long-distance high throughput low latency data links, which are hard to establish in remote areas and a highly contested IEW (Information and Electronic Warfare) environment[17]. On the other end of the computation spectrum are the promises given by another technology, that of Edge Computing.[18] The difference is in the place where computation is being carried out. In this case, it is as close to the place where data is being generated. Such a concept can be applied to sensors that do not suffer from limitations imposed by size, weight and power. Pre-processed or presentable data can therefore be transmitted to the end user, thereby shrinking data processing times as well as the overall quantum of data to be transmitted.[19] Edge Computing is being extensively used in the Space domain, with India-based Space startups like KaleidEO and SkyServe demonstrating such capabilities.

New and transformative architectural technologies like Cloud Computing and Edge Computing have their inherent advantages. Their applicability to the needs of military battle networks will vary across domains. Since the panacea is yet to be found, data optimisation will be the key to the 'Data Centric' approach to military networks.[20]

Data: A Joint Strategy

Large datasets generated by today's digital platforms become a strategic asset. Its sovereignty, standardisation, security, storage and exploitation as per the needs of the country therefore assume great importance. In the Armed Forces, thousands of gigabytes of digital data is generated every day by various sensors and weapon platforms. Irregular storage management, insufficient format standardisation, undefined data access protocols and lack of data accountability may lead to a large amount of this crucial data being lost. There may be a lack of recognition across the Armed Forces that data is important. Data is a critical component of all analytical tools, Machine Learning (ML) algorithms and AI-based software. Predictive modelling based on Neural Networks, where pattern recognition is the key, requires a large amount of training data. Quality of data also plays a crucial role in providing high assurance rates to predictive modelling. Hence, digital data archiving, storage, format standards and quality, all become important.

Interoperability of battle networks is a crucial area which the Armed Forces must consider holistically. Interoperability has costs associated with it. Interoperability will require data standardisation across sensors, shooters, backend servers, processing units, networks and more, which eventually may not be feasible. However, interoperability is not binary. It is possible to define the degree of interoperability.[21] It will also be worthwhile to understand that interoperability at different levels of the network will have different challenges. Data sharing at the backend will be fundamentally different from data sharing at the tactical edge. Hence, the Armed Forces may look at data-specific access protocols instead of an overly ambitious all-out interoperability.

Interoperability of Defence Communication is another emerging data-driven environment. With the ubiquitous presence of digital communications, Armed Forces across the globe are now opting for Software Defined Radios (SDR). These SDRs have inherent flexibility, interoperability, security and spectrum efficiency advantages.[22] In India too, Armed Forces across the domains are procuring SDRs as per their service needs. Indigenisation of SDRs is also underway at Defence Research and Development Organisation (DRDO). SDR technology requires a standardised operating software environment and associated applications, known as waveform. Portability and interoperability among the SDRs are only possible with such standardisation[23].

With so much reliance on data and its associated networks, Counter Battle Network Operations are going to be the first among the target list of the adversary's most probable Courses of Action (COA). Armed Forces therefore need to formulate strategies to mitigate the effects of both the kinetic and non-kinetic weapons that the adversary may employ actions against their battle networks. However, this threat perception must not lead to actions bordering paranoia. An overly sensitive approach to the security and secrecy of data and networks becomes counter-productive to battlefield efficiency. It is therefore important to segregate data and networks according to their merit. Encryption standards across networks must therefore vary depending on the data type, thus enhancing the required degree of interoperability for non-critical data.

United Kingdom Ministry of Defence in their document titled 'Data Strategy for Defence' describe data as their second most important asset, only behind their People. Consequently, this document describes the journey to formulate 'rules of the road' for Defence related data.[24] The US Dept of Defence (DoD) has also come up with its own DoD Data Strategy. The key focus areas of the document are Joint All Domain Operations, Decision support to Senior Leadership and Business Analytics. It aims to make defence data visible, accessible, interoperable, trustworthy and secure.[25]

Indian Armed Forces also need to formulate a Joint Defence Data Policy framework. This framework should include Defence Data Management Strategy, Defence Data Network Protocols, Defence Data Encryption Standards, Defence Data Storage and Retrieval Policy, Defence Data Analytics and AI Tools Application Protocols, to name a few. These can flow from an overarching Defence Data Strategy. Such a document can become the guiding light for future ICT procurements, networking and software designing, defence industry standards for partnership, collaborations, and even promoting indigenization.

Data: The India Way

The Ministry of Electronics and Information Technology (MeitY), under the Government of India (GoI), is entrusted with the issuance of data policies in the public domain. Consequently, the Ministry has issued the India Data Accessibility and Use Policy in 2022.[26] For data management, the Ministry has announced the setting up of the India Data Office (IDO). For data management, each ministry is to nominate a Chief Data Officer, who in turn will be responsible for the implementation of policy, data access and sharing, data quality and metadata standards. This policy, along with the National Data Governance Framework Policy, aims to provide the much-needed standardisation and allocate responsibility for data management across ministries under GoI. However, the real success story of Digital India has been the combined power of UIDAI (Unique Identification Authority of India), open APIs (Application Programming Interfaces) and UPIs (Unified Payment Interfaces), which together have transformed the digital landscape of the country[27]. This is an apt example of how to set up required digital protocols under a policy framework, provide centralised regulation, while at the same time, allowing enough latitude for public-private innovation to be fostered.

The Ministry of Defence (MoD) has also taken certain positive steps in this direction. To enable waveform interoperability among SDRs provided by various vendors, the Ministry has developed a reference implementation of India specific operating environment called India Software Communication Architecture (SCA) profile or Indian Radio Software Architecture.[28] Artificial Intelligence has been given a big push by the formation of the Defence AI Council (DAIC). Consequently, a list of AI-based products that can be tailored exclusively for Defence needs has been created. Both public and private companies are being encouraged to partake in the development of AI-based products for Defence.[29]

In the past few decades, the Indian Armed Forces have been trying to achieve Net-Centricity. Since 2010, The Indian Air Force (IAF) has created its secure pan-India networks in the form of AFNET. The Integrated Air Command and Control System (IACCS) that also rides on AFNET has undergone various upgrades and today supports one of the most robust and secure Air Defence (AD) architecture. The Indian Navy has been constantly upgrading its Trigun Network to achieve Maritime Domain Awareness (MDA) by integrating various inputs from coastal surveillance radars, Automatic Identification System (AIS) equipped vessel data through satellites, and vessel traffic management systems, among others.[30] Under project Akash Teer, the Indian Army aims to integrate all its sensors and shooters through a network.[31] While service-specific Net-Centricity is being achieved rapidly, interoperability is on the back burner.

To overcome this shortcoming, a tri-service Defence Communication Network (DCN) is being established.[32] However, by adding another network layer, the problem of interoperability of networks and cross-domain data access remains as it is.[33] The fact of the matter is that interoperability of networks and seamless data transfer is a worldwide challenge, with leading militaries like that of the US still grappling with it. Many of their previous efforts, like the Joint Tactical Radio System (JTRS) and Joint Enterprise Defence Infrastructure (JEDI) went awry.[34] Despite the buzzwords of MDO and JADC2, even today, each of their services continues to pursue independent service-specific network solutions. Hence, the Indian Armed Forces must quickly abandon an overambitious approach to cross-domain transmissivity. Instead, a more pragmatic approach is advocated.

One such pragmatic approach involves nominating a 'Lead Service'. This lead service is to formulate the standards of network protocols, encryptions and security across all domains within the Armed Forces. Such an approach will benefit from the existence of an already established IT infrastructure, a networking architecture, a trained human resource, and institutional experience in the implementation of policies, thereby reducing costs and accelerating success. While following such an approach, however, the lead service needs to take cognizance of the domain-specific needs of other services and must be able to tailor its network accordingly. Here, it is suggested that the well-established net-centricity of the IAF or any other service can be harnessed to conceptualise a tri-service data cloud and network protocol of cross-domain connectivity. The end-point data connectivity to remote users across domains may be provided by using secure WiFi networks and Satellite links. Also, as has been mentioned earlier, services must jointly choose which data needs to be shared within the sub-layers of the network, thereby optimising the data bandwidth requirements of the entire network. Domain-specific Net-Centricity efforts must be continued concurrently.

Along similar lines, another practical approach may involve nominating a ‘Lead Command’. Since the contours of the Joint Commands have started to emerge, one among the newly formed Joint Theatre Commands can be entrusted with the task of quick implementation of a new Joint Network. Defence Cyber Agency (DCyA), under Headquarter Integrated Defence Staff (HQ IDS) can help in this endeavour. Thus, the Lead Command becomes the test bed for creating a larger tri-service interoperable network in the near future. A *de-novo* approach that leverages existing data science technologies and ICT expertise, available through public-private collaboration, can produce exciting results. Implementing modern data management concepts based on cloud computing and edge computing in the short term, and wideband wireless networks and Space-based LEO constellations in the long term, can be used to meet the data needs of the ‘digital’ soldier/ sailor/ airmen.

Conclusion

So far, it has been discussed that in war, it is not always the newest technology that provides the edge to one side. At times, it is the amalgamation of several existing technologies that can create conditions necessary for victory. With terms like Data-Centricity, Multi-Domain Operations and Informationised War entering the military lexicons, more is being demanded from data and their battle networks. Data management in the Armed Forces needs urgent attention. It will be the lifeblood of many emerging technologies. Formulating a Joint Data Strategy is a good approach to data management across all domains. The success of Digital India has provided the much-needed ray of hope in formulating a nuanced Defence Data policy. Indian Armed Forces must abandon the over-ambitious tri-service integration of networks. Instead, a more pragmatic approach needs to be taken. With the formation of Joint Structures in the Indian Armed Forces moving from the planning to implementation stage, the jointness in ‘hearts and minds’ needs to progress to jointness in ‘bits and bytes’.

*****

Gp Capt Ankur Mathur was commissioned in the Fighter stream in June 2001. He has 2600 hours of flying experience on various fighter aircraft like MiG 21, MiG 29 and Hawk Mk 132. He is Qualified Flying Instructor and an alumnus of Defence Service Staff College, Wellington. He has undergone Higher Air Command Course and Warfare and Aerospace Strategy Program at College of Air Warfare. He is presently posted as Chief Operations Officer of an operational base in Eastern Air Command.

NOTES

[1] John Keegan, A History of Warfare, (Pimlico ed. 2004), pp 38,161,328

[2] Peter H. Diamandis & Steven Kotler, The Future is Faster than You Think, (Simon & Schuster,2020).

[3] Hamish McRae, The World in 2050, (Bloomsbury Publishing, 2022), pp 139-141

[4] www.investopedia.com, "What Is Moore's Law and Is It Still True?", available at https://www.investopedia.com/terms/m/mooreslaw.asp, accessed on 03 Jun 24.

[5] RAND Corp, "What Is JADC2, and How Does It Relate to Training?", available on https://www.rand.org/pubs/perspectives/PEA985-1.html, accessed on 03 Jun 24.

[6] Paul B. Symon and Arzan Tarapore, "Defense Intelligence Analysis in the Age of Big Data", (Issue JFQ 79, October 2015, National Defence University Press), available on https://ndupress.ndu.edu/Media/News/Article/621113/ defense-intelligence-analysis-in-the-age-of-big-data/, accessed on 03 Jun 24.

[7] István Szabadföldi, "Artificial Intelligence in Military Application – Opportunities and Challenges", (Land Forces Academy Review Vol XXVI, No.2(102), 2021), available on https://sciendo.com/article/10.2478/raft-2021-0022, accessed on 03 Jun 24.

[8] Sydney J. Freedberg Jr., "Artificial Stupidity: Learning To Trust Artificial Intelligence (Sometimes)", (2017, Breaking Defense), available on https://breakingdefense.com/2017/07/artificial-stupidity-learning-to-trust-the-machine/, accessed on 03 Jun 24.

[9] John A. Warden, III, The Air Campaign: Planning for Combat, (toExecl,2000), pp 13

[10] Peter W. Mattes, "Systems of Systems: What, Exactly, is an Integrated Air Defense System?", The Mitchell Forum (No 26, June 2019), available on https://mitchellaerospacepower.org/wp-content/uploads/2021/02/a2dd91_2f17e209f90f4aaab80b116e4d139eb4.pdf, accessed on 03 Jun 24.

[11] Todd Harrison, "Battle Networks and the Future Force: Part 1", (Center for Strategic & International Studies, August 2021), available at https://aerospace.csis.org/battle-networks-and-the-future-force/, accessed on 04 Jun 24.

[12] Max Polyakov, "The Future of Starlink: Hidden Military Potential", (Max Polyakov News Space, August 2023), available at https://maxpolyakov.com/hidden-military-potential-of-starlink/, accessed on 04 Jun 24.

[13] https://www.geeksforgeeks.org/cloud-computing/, accessed on 04 Jun 24.

[14] News report, "NATO selects Thales to Supply Its First Defence Cloud for the Armed Forces", (Express Computer, Jan 2021), available at https://www.expresscomputer.in/news/nato-selects-thales-to-supply-its-first-defence-cloud-for-the-armed-forces/72213/, accessed on 04 Jun 24.

[15] DoD Cloud Strategy, 2018, available at https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF, accessed on 04 Jun 24.

[16] US Army's The Army Cloud Plan (2020), available on https://api.army.mil/e2/c/downloads/2020/09/11/81bb912e/the-army-cloud-plan-2020-final2.pdf, accessed on 04 Jun 24.

[17] Todd Harrison, "Battle Networks and the Future Force: Part 1", (CSIS) pp7

[18] Stephen J. Bigelow "What is edge computing? Everything you need to know", available on https://www.techtarget.com/searchdatacenter/definition/edge-computing, accessed on 04 Jun 24.

[19] Todd Harrison, "Battle Networks and the Future Force: Part 1", (CSIS) pp 6-7

[20] Jerome Dunn, "What "Network-Centric to Data-Centric" Really Means", (Booz Allen Hamilton), available on https://www.boozallen.com/insights/defense/defense-leader-perspectives/what-network-centric-to-data-centric-really-means.html, accessed on 04 Jun 24.

[21] Todd Harrison, "Battle Networks and the Future Force: Part 2", (Center for Strategic & International Studies, November 2022), pp 6, available on https://aerospace.csis.org/battle-networks-and-the-future-force-part-2/, accessed on 04 Jun 24.

[22] Dinesh Kumar Pandey, "Software Defined Radio: Enhancing Communication Capabilities", https://capsindia.org/software-defined-radio-enhancing-communication-capabilities/

[23] News report, Economic Times, "Defence ministry accords high priority to Indigenisation of Software Defined Radios",(26 July 2022), available at https://government.economictimes.indiatimes.com/news/technology/defence-ministry-accords-high-priority-to-indigenisation-of-software-defined-radios-for-armed-forces/93130708, accessed on 04 Jun 24.

[24] UK Ministry of Defence, Data Strategy for Defence (2021), available at https://assets.publishing.service.gov.uk/media/614deb7a8fa8f561075cae0b/Data_Strategy_for_Defence.pd, accessed on 03 Jun 24.

[25] US DoD, DoD Data Strategy 2020, available at https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF, accessed on 04 May 24.

26 India Data Accessibility and Use Policy, (MeitY ,GoI, 2022), available at https://www.meity.gov.in/writereaddata/files/India%20Data%20Accessibility%20and%20Use%20Policy.pdf

27 Divya Goel, "From Platforms to Protocols: India's Story of Leapfrogging Financial Inclusion ", (MEDIUM, 2022), available on https://medium.com/digitalhks/from-platforms-to-protocols-indias-story-of-leapfrogging-financial-inclusion-c5c127ec57a2, accessed on 04 Jun 24.

28 PIB Delhi, "Aatmanirbhar Bharat': MoD accords high priority to indigenisation of Software Defined Radios for the Armed Forces", (26 Jul 2022), available at https://pib.gov.in/PressReleasePage.aspx?PRID=1844825

29 Dept of Defence, MoD India, "AiDef" (2022), available at https://www.ddpmod.gov.in/sites/default/files/ai.pdf, accessed on 04 Jun 24.

30 Anil Chopra, "Towards an Integrated Military Future", (Anirveda,2021), available at https://raksha-anirveda.com/towards-an-integrated-military-future/, accessed on 04 Jun 24.

31 Ibid

32 Ibid

33 Sunil Srivastava, "JOINT C4ISR FOR THE INDIAN ARMED FORCES- QUO VADIS?", (CENJOWS, Vol I, Issue 1, O t 2022), available at https://cenjows.in/wp-content/uploads/2022/10/1-Joint-C4ISR-for-The-Indian-Armed-Forces-by-Lt-Gen-Sunil-Srivastava-Retd.pdf, accessed on 04 Jun 24.

34 Ibid, pp 6