

CENTRE FOR JOINT WARFARE STUDIES



CENJOWS

**JOINT WAVEFORM
INTEROPERABILITY
SYSTEM (JOWIS) – COMMON
TACTICAL DATA LINKS FOR
THE FORCE OF 21ST
CENTURY**



Lt Col Vivek Gopal, a graduate of the National Defence Academy, was commissioned in December 2000. A MTech, paratrooper & certified Project Management Associate, the officer is presently posted as Instructor at a premier training establishment.

DISCLAIMER: DATA USED FOR THIS BRIEF IS SOLELY BASED ON OPEN SOURCE ACCESS/ OSINT & CREDIBILITY OF THE INFORMATION PRODUCED IS AS GOOD AS THE CITED SOURCE; BEING VERY FEW IN OPEN DOMAIN OWING TO THE NATURE OF THE TOPIC.

THE ABBREVIATION **JoWIS** IS AN ACRONYM COINED BY THE AUTHOR AS HYPOTHESIS.



(**Source:** Source: Data Link Solutions - Link 16 TacNet™ Tactical Radio. (2021). Datalinksolutions.net.
<http://www.datalinksolutions.net/products/tacnet-radio.php>)

Abstract - Evolving threats of the modern day battlefield are characterized by swift operations, battlefield transparency & a combat pulse which is an amalgamation of overwhelming force being applied at the point of decision. This has been made possible due to the advances in technology which provides near real-time information to the commanders, shortening the Observe-Orient-Decide-Act or OODA loop & thereby the sensor to shooter kill cycle. This real time information rides over a network of networks linking geographically dispersed entities sharing information over data links, thereby providing situational awareness. These data links need to be shared among the services to ensure the forces act on a Common Operating Picture. Data link networks & the main communication backbone, therefore, need to be interoperable. Carrying a plethora of information, these data links need to have advanced capabilities in terms of the information payload as well as the survivability characteristics in a communication degraded environment. Various nations in the world have developed or are in the process of developing new data links or using the existing ones to achieve jointness of effort. However, despite the number of links in use, interoperability among these remains to be developed – to arrive at a Common Data Link which will enable all assets (weapon platforms) to operate & exchange real-time information. While the US Forces & NATO have been leading in this field, India too has made a start, albeit late. As we inch towards adopting new technology to be fused into warfare, this is the right time to explore the feasibility of a Common Data Link; a **Joint Waveform Interoperable System of JoWIS** which can form a part of new systems being inducted as well as retain the capability to integrate with legacy systems already in use.

Keywords– Datalink, TDL, Link 11, Link 16, Link 22, JREAP, SIMPLE, NEWN, AFNET, Trigun, IACCS, C4ISR, NCW, NCO, EBO

Introduction

Network-centric by its name is an oxymoron – networks being ‘centre-less’, hence a network; however, the forces are proponents of the Metcalfe’s law¹. Tactical Data Links or TDLs are inseparable from Network Centric Operations or Warfare (NCO/ NCW); in fact the former serves as the enabler for the latter. The present brief also covers the aspects of NCW & addresses the issues with reference to TDLs & their importance especially in terms of interoperability which is at the core of NCW. To arrive at a Common Operating Picture (COP), there is a need for all the tactical elements to ‘talk to each other’ as it is this shared awareness that brings out the essence of Effect Based Operations or EBO, which is, overwhelming superiority over the adversary. To be able to ‘Strike Before He Thinks’ requires the three services or the triad to leverage this information to an advantage using all means at hand & finally utilize the most optimal package at the point of decision. To tide over the interoperability issues, a Common Data Link across the entire services network called Joint Waveform Interoperability System or JoWIS is proposed.

This brief delves into the aspect of TDLs & how a common data link is inescapable to promote jointness of operations. Technical details have deliberately been left out to limit the scope of this brief. For the readers of interest, detailed analysis of the data links is available as reference to this brief.

Network Centric Operations – Foundation for Jointness

Network Centric Operations (NCO) or Network Centric Warfare (NCW) is a key component of the armed forces based on shared perspective or a common operating picture (COP) arrived at by use of computer & communication networks working in tandem. The Joint Doctrine of the Indian Armed Forces in 2017 as well as the Land Warfare Doctrine later in 2018 both have highlighted the aspects & inescapability of Command, Control,

¹“Metcalfe’s Law, named after Robert Metcalfe, the inventor of Ethernet and founder of 3Com Corporation. It was a phenomenon first observed in commercial communications as Metcalfe sought to address the problem of creating larger networks out of many smaller ones. The law contends that the power of a network increases with the square of the number of nodes connected to the network. Network-centric warfare advocates build on this law by asserting that maximizing the number of nodes increases the chances of realizing the promise of networks through ubiquitous connectivity and interoperability.” (*Anatomy of Network-Centric Warfare*. (2004, May 18). SIGNAL Magazine. <https://www.afcea.org/content/anatomy-network-centric-warfare>)

Communications, Computers, Information, Intelligence, Surveillance & Reconnaissance (C4I2SR).ⁱ Three fundamental questions that always arise are – interoperability of the systems of different services, limited bandwidth available & threats posed to the cyber-systems in a growing dependence on networks. However, a dependence on NCW is the key to defence transformation as well as to ensure that we operate from a position of overwhelming advantage, if not asymmetry, in a futuristic hostile situation. With the growing importance of NCO which may also serve as a deterrent, the objectives can be stated as:-

- Self-evolving & self –synchronized system development
- Ability to reach a COP in shorter time frames – reduce reaction time or take a proactive stance
- Tap into a joint or collective knowledge of the situation on ground to enable furtherance of overall aim

Although there are proponents of the theories concerning over-dependence on ‘information’ for warfare, the aim of this brief is not about weighing the benefits of NCW against its disadvantages or vulnerabilities. Here, we are merely trying to understand the ways & means of establishing a nationalized cross-domain information grid within which the assets are networked using a common data link system which is hypothesized as JoWIS. The importance of NCW has also been studied which reflects the shortening of the OODA cycle.

“In traditional military operations, a mission is assigned and planned, forces are generated, and operations are executed to concentrate power on an objective. This is a highly coordinated, “stepped” cycle (see Fig.1 below): periods of relative inaction, during which forces are generated and actions coordinated (the flat part of the step) alternate with periods of action, when combat power is applied (the vertical part). However, if forces were networked to create a near-real-time situational awareness, then we could act continuously along a relatively smooth “combatpower curve.” We would no longer need to pause before deciding on further action; the information and coordination needed would already be there. The shared situation awareness promised by network-centric operations would also permit a flattened decentralized command structure in which decisions could and would be made at the lowest practicable level of command. Combined with self- synchronization, it would permit us to reclaim the “lost combat power”ⁱⁱ

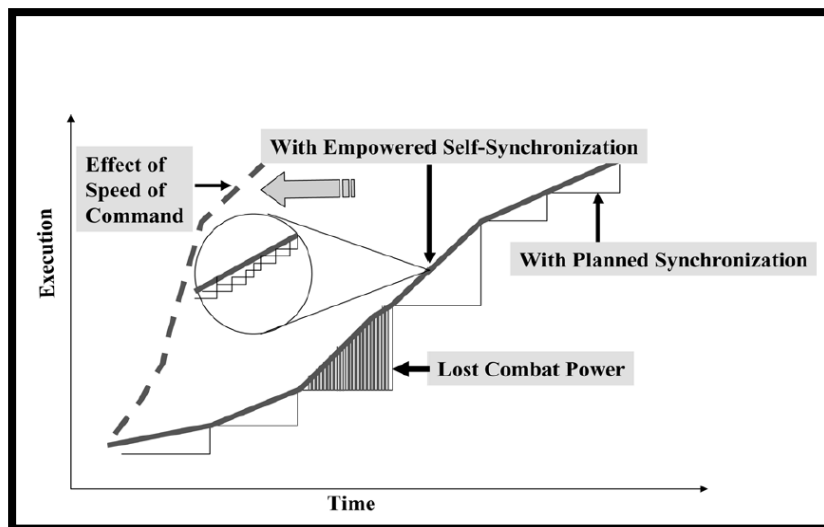


Fig.1 - Self-synchronization & Speed of Command: Effect of Networked Operations

(Source: http://www.dodccrp.org/files/Smith_EBO.PDF)

History of Data Links

World War II (WW2) veteran & code breaking expert Gordon Welchman can be described as one of the founding fathers of modern-day Tactical Data Links. He was subsequently overshadowed by the fame of colleague Alan Turing. A maths genius Welchman & Turing were both responsible for cracking of the Nazi Enigma code which led to the code-breaking & Allies were able to decipher key German secret messages during the war.

Welchman subsequently moved to America and developed the Joint Tactical Information Distribution System (JTIDS) – the military communications TDL system still in use today in the United States (US) and with North Atlantic Treaty Organisation (NATO) forces. JTIDS supports data communications in air, surface and land using Link 16, a popular tactical data link.

The work done by Welchman was so important that Churchill designated it as 'Ultra-Secret' & that it should remain classified at all cost. The complex cryptanalysis technique deciphered a plethora of information despite the message string remaining unbroken. This technique is still in use by the NATO forces.

Polish cryptanalysts had also developed 'Bomba', an electromechanical device which could find the Enigma settings used by German operators. The Polish design was further improved upon by Welchman after the machine was smuggled into Britain. Another outstanding invention by Welchman was the 'Diagonal Board' which was more powerful than the 'wheel setting' used by the Germans to randomly program their Enigma machines.

After obtaining US citizenship in 1962, Welchman joined the MITRE Corporation, working on secure JTIDS communication systems for the US military. He developed the Time Division Multiple Access (TDMA) algorithms for frequency hopping and cipher protection. JTIDS was sponsored by the Air Force Electronic Systems Division (ESD). A book² authored by Welchman created a furore in which he described the war time activities of code breaking. Welchman died in 1985, however, his work was also published as a paper³ in 1986.

Understanding a Tactical Data Link

Sharing a common data link is a pre-requisite for all sensors & weapon platforms on the ground, sea or air to be able to share information. Tactical Data Link (TDL) is the means to disseminate processed information from Radars, Electronic Warfare (EW), Identification Friend or Foe (IFF), Sonars and information related to various combat functions between the far-fighting units on a battlefield. TDL exchanges digital information on a near-real-time basis over a common network, with the tactical data updated continuously and automatically by each of the nodes. The information provides the common approach to various systems & operating environments. The information moves on this data link & hence the developed data link should be future-proof; capable of supporting future generation weapon platforms securely. Managing, exploiting & there after extracting & disseminating data over the information layer is what is of prime importance. Various data links that are being used as part of existing tactical communication systems has been listed as **Appendix 'A'** to this brief.

While planning to deploy a TDL, it is important to plan & define our space not only in terms of length, height and width, but based on the operating volume which will be a function of the range, area, altitude and time domains.

Range – Depending on what distances are the various employed assets going to operate is crucial. Radio frequency (RF) characteristics are a function of the distance of operation as well as the electro-magnetic & surrounding environment. For line of sight (LOS) communication we may depend on Ultra-high frequencies (UHF) or Very high frequencies (VHF). For non- LOS cases, we may have to rely on waveforms riding on satellite links or airborne/ ground relays.

²Welchman, G. (1982). The Hut Six Story: Breaking the Enigma Codes.

³Gordon Welchman (1986) From Polish Bomba to British Bombe: The birth of ultra, Intelligence and National Security, 1:1, 71-110, DOI: [10.1080/02684528608431842](https://doi.org/10.1080/02684528608431842)

Area – Range helps us in determining the type of waveform & frequency of operation selection. Area, similarly, helps us determine the architecture that will have to be in place to generate the COP. We might have a single point of reception for air to ground communication. However, when mingled with early warning elements, local intelligence assets (Radars for example), will need a network of relays to disseminate the same information to as many nodes.

Altitude – This factor can be seen as the range function in a vertical orientation. The data link should not suffer due to multi path effects or terrain masking.

Time - This factor is based on the weapon platform being used. Land & naval vessels may operate continuously during day & night. Airborne platforms may only be available for a short duration based on the operations envisaged. How quickly can the information be passed over the links established i.e. the time-sensitive nature is thus also important while deciding the link.

As the number of links with varying characteristics are utilised, planning the operation with as many interfaces also become pertinent. After the factors mentioned above are decided, we can move on to designing the network. This will involve simulation of the various data link capabilities of the platforms being pressed into action. Extensive use of a 'Link Planning Simulation & Management Tool'⁴ is inescapably required to plan the same. It is with this tool that one will be in a position to decide the way information will be received by the platforms, disseminated, collected & collated, limited by the data link capabilities⁵.

Various TDL standards as evolved by NATO forces & comparison of some of the standards are listed as **Appendix 'B'** & **Appendix 'C'** to this brief respectively.

Data Links Used in Different Nations

The aim behind network-enabled military capabilities is to collect, process & distribute information across several domains & multiple platforms in a Battlefield Internet of Things (IoT). Using TDLs enables the users to cooperate & collaborate using various computing devices & gain a decisive overall advantage over the adversary. There are several interoperability

⁴Refer iSMART - interoperable Systems Management and Requirements Transformation document suite. iSMART supports a suite of documents which define the TDL requirement in a hierarchy. iSMART is an open process that can be employed by any organization to assist in the management of interoperability.

⁵This has been stated very simplistically. The planning will be time consuming & very deliberate as it will have to take into account assets which will 'come-and-leave' the network. Redundancy planning as well as contingency nodes etc all has to be planned & simulated.

(Source: TACTICAL DATA LINK – FROM LINK 1 TO LINK 22. (2016). *Scientific Bulletin of Naval Academy*, 19(2). <https://doi.org/10.21279/1454-864x-16-i2-046>)

Link type	User community	Application
Link 1	Aerial situation	Interfaces with other networks (aerial control/ aerial defense), with mobile systems and with the primary users group.
Link 11	Marine control Aerial control	Provides tracking data exchange for image compilation and transmission of orders in the C2 domain.
Link 11B	Aerial defense	Tactical information exchange between soil-based weapon systems, C2 and surveillance systems and Link 11 network participating units.
Link 16	Joint	High-throughput digital data link, without a nodal point (hub), which includes EPM for engaging a multiple combat environment (terrestrial, naval and aerial combat)
Link 22	Joint	Designed for ensuring connectivity outside the direct line-of-sight (BLOS), using DTDMA architecture.

Fig. 3 - TDLs – Application Scenarios

(Source: TACTICAL DATA LINK – FROM LINK 1 TO LINK 22. (2016). *Scientific Bulletin of Naval Academy*, 19(2). <https://doi.org/10.21279/1454-864x-16-i2-046>)

TDLs help to achieve a joint picture to the commanders which assists in the execution of the operation with precision based on accurate & real time information. This also serves as the basis for the design of the typical protocols customized to suit the requirement. As brought out above, the TDLs to be used in the case of joint operations are the Link 16 & Link 22. The networking scheme characteristics of the various TDLs are covered below as Fig. 4.

Characteristics	Link 1	Link 11	Link 16	Link 22
Frequency	Point-to-point land line	HF/ UHF	UHF/ Spread	HF/UHF Spread
Speed (bit/sec)	1,200	1,800	> 57,600	-
ECM resistance	-	-	x	x
Crypto-secure	-	x	x	x
Nodeless	-	-	x	x
Extended LOS	-	-	x	x
Antijam	-	-	x	-
Data rate (kbps)	1.2	1.3 ÷ 2.25	2.8 ÷ 115.2	2.4
Standard message	S-series	M series	J series	J series
Participants		4 ÷ 8	> 128	40
Voice circuits	-	-	2	-
Architecture	Duplex digital	Radio Broadcast	TDMA	DTDMA

Fig. 4 - TDL Architectures

(Source: TACTICAL DATA LINK – FROM LINK 1 TO LINK 22. (2016). *Scientific Bulletin of Naval Academy*, 19(2). <https://doi.org/10.21279/1454-864x-16-i2-046>)

Covering all the data links will exceed the scope of this brief. However, the important links which operate for joint operations are the ones we should be looking at to promote the development of similar protocols to achieve the aim of jointness.

Link 16or TADIL- J or Tactical Digital Information Link –J- This is a high-capacity datalink, with frequency hopping features and anti - electronic counter-measure capabilities (Anti-ECM). Link 16 uses Joint Tactical Information Distribution System (JTIDS) terminals and Multifunctional Information Distribution System (MIDS). Link 16 has implemented the Time Division Multiple Access (TDMA) technique, that provides 128 time slots/second for the various users. The time slots are organized in several functional groups of network users.

Unlike Link1 and Link 11, Link 16 uses encrypted high-capacity datalink, with a mesh network, and provides electronic protection measures for fully-operational communications in combat situations (air, terrestrial, sea). Enhanced communication capabilities are provided by Link 16 & assists in the real time tactical information exchange. The salient features include nodelessness, anti-ECM, increased throughput, small form factors for use in aerial platforms, secure voice & precise position indication. Utilising LOS principle the various Link 11 terminals are the JTIDS (1st and 2nd generation equipment), Multifunction Information Distribution System (MIDS) Low volume terminals (LVT) series 1 to 11 for various platforms & MIDS JTRS which is the Joint Tactical Radio System. A point to note here is that while Link 16 refers to the whole network, JTIDS is the communication component of the network.

Link 22 – With features similar to Link 11, this TDL enables BLOS (Beyond Line of Sight) communication capabilities, so in the HF band Link 22 is able to provide communications up to 300 nautical miles. Link 22 scores over other systems in being operable even in inclement weather conditions by working at a lower data rate. Redundancy is built-in – if a specific unit fails, the whole network is not affected because of the distributed protocols usage. The protocol stack of Link 22 & a comparison with Link 16 is shown below as Fig. 5 & a comparison between Link 11 & Link 22 shown at Fig 6.

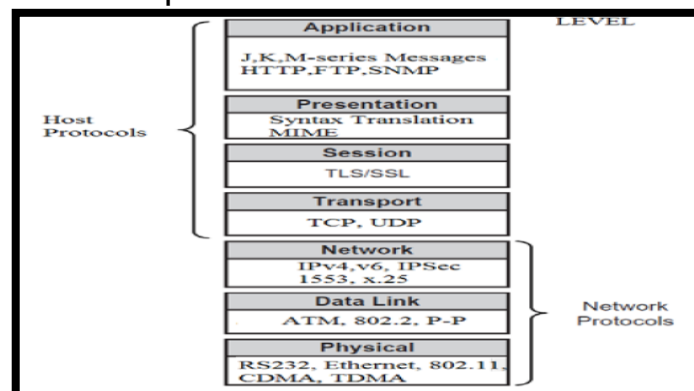


Fig. 5 - Protocol Stack for Link 22

(Source: TACTICAL DATA LINK – FROM LINK 1 TO LINK 22. (2016). *Scientific Bulletin of Naval Academy*, 19(2). <https://doi.org/10.21279/1454-864x-16-i2-046>)

Function/ Specification	Parameters/Advantages/Limitations	
	Link 11	Link 22
Network Access	<ul style="list-style-type: none"> - Increased net cycle times - Large access delay 	<ul style="list-style-type: none"> - TDMA access - Prioritization of messages feature
Emergency calls	<ul style="list-style-type: none"> - No options 	<ul style="list-style-type: none"> - Priority Injection feature
Capacity	<ul style="list-style-type: none"> - Limited number of participants (62) 	<ul style="list-style-type: none"> - More units (125)
Area of Operation (Network Coverage)	<ul style="list-style-type: none"> - Limited area - Dependence of the platforms and their positions - Units must be all connected with the NCS 	<ul style="list-style-type: none"> - No limitation (it uses the WGS-84 System); - Increased area of operation; - Flexible network; - LOS and BLOS capabilities; - Routing&relay protocols.
Communication Security	<ul style="list-style-type: none"> - Low encryption level - Weak security. 	<ul style="list-style-type: none"> - Strong encryption system. - Strong security.
Transmission Security	<ul style="list-style-type: none"> - Fixed HF or UHF frequencies; - Jam vulnerabilities. 	<ul style="list-style-type: none"> - Frequency hoping solutions provide reliable communications; - Fixed frequency communications are not so affected as Link 11 because of the multiple networks
NCS failure	<ul style="list-style-type: none"> - If NCS is down the entire network will be affected 	<ul style="list-style-type: none"> - No NCS required - No single point of failure
Reliability	<ul style="list-style-type: none"> - Bad conditions could affect the transmission - Limited waveforms availability 	<ul style="list-style-type: none"> - Special mechanism for bad transmission conditions - More robust waveforms
Bandwidth	<ul style="list-style-type: none"> - Limited Bandwidth - Transmission rates from 1,090 bit/s to 1,800 bit/s 	<ul style="list-style-type: none"> - Wider Bandwidth - Transmission rates from 1,493 bit/s to 12,666 bit/s

Fig. 6- Comparison Between Link 16 & Link 22

(Source: TACTICAL DATA LINK – FROM LINK 1 TO LINK 22. (2016). *Scientific Bulletin of Naval Academy*, 19(2). <https://doi.org/10.21279/1454-864x-16-i2-046>

JREAP – Joint Range Extension Application Protocol - Enables tactical data to be transmitted over larger distances. Capabilities include extending the range-limited tactical networks to beyond LOS (BLOS) while reducing their dependence upon relay platforms, reducing the loading on stressed networks, providing backup communications in the event of the loss of the normal link, and providing a connection to a platform that may not be equipped with the specialized communications equipment for that TDL.^v JREAP software can be integrated into a host system or into a standalone processor. The appropriate interface terminals are required at each end of any JREAP alternate media link. (refer Fig. 7)

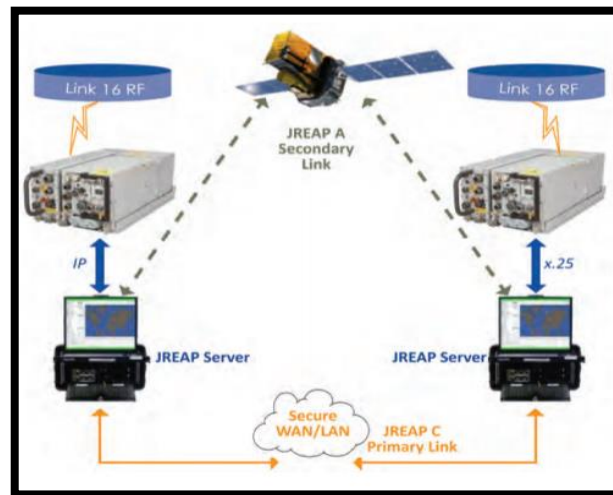


Fig. 7 - Implementing JREAP
(Source: TDL Technology Magazine, 2017)

JREAP & Standard Interface for Multiple Platform Link Evaluation or SIMPLE are both used when TDLs are to be linked beyond the normal communication limits. JREAP relies on encapsulation of data with the JREAP wrapper, so BLOS communication can take place with those platforms which are not even equipped with Link 16 equipment. On the other hand, SIMPLE is not used in the operational environment & is used to transmit between geographically dispersed test environments.^{vi}

China

Not much information is available as OSINT with respect to the data links planned to be used or already in use for the PLA. However, inference can be drawn with respect to the impetus being given to 'informatization' as a key player towards force upgradation.^{vii}

"Without informatization, there is no modernization."

- Xi Jinping during the inspection of the Hainan Provincial Government Affairs Data Centre, 13 April 18.

Apart from the focus on informatization, the Chinese are working on development of the 'tactical internet' which can link various units together.^{viii} The Chinese are well aware of the various Data links in use by the US forces. They have reiterated the resolve to develop strategic advantage over the adversary by the following tenets^{ix}: -

- Strengthen strategic planning
- Speed up the construction of networks
- Promote technological innovation
- Promote collaboration between civil & military

Military use of the 'cloud' has also been expressed as an area of interest by the Chinese.^xNeedless to say that the Integrated Network & Electronic Warfare INEW roadmap of the Chinese is sure to keep pace with the developments as are taking place with rest of the leading nations, more so, when China is investing heavily in satellites to build a robust all round capability. For system-of-systems integration [tixironghe, 体系融合], the PLA (read Strategic Support Force or SSF) will need not only to integrate these systems together but also seamlessly feed this information into force-wide networks such as the Integrated Command Platform [yitihuazhihuipingtai, 一体化指挥平台] to support both strategic missions and theatre command operations.^{xi}

Pakistan

Like other modern militaries, the Pakistani armed forces also boast of C4ISR capabilities. The most visible elements of Pakistan's C4ISR network include the 'Erieye' and 'Karakoram' Eagle Airborne Early Warning & Control (AEW&C) systems. Although the capabilities are shrouded in secrecy, hints & OSINT suggest mention of a national data-link solution. Pakistan's C4ISR system could be seen as an implementation of core technologies, particularly ISR and communications.

The Pakistani military makes use of multiple data-link protocols. Details in open source are very few, however an estimate based on how the PAF operates can throw some light on to the TDLs architecture. The PAF's primary TDLs are the Link-16 MIDS-LVT (Low Volume Terminal) which it supposedly claims as indigenously developed.^{xii} (Ref Fig. 8)

The earliest official record of the 'National Data Link' occurred in 2010-11 when the indigenous data-link solution was listed by the Ministry of Defence Production (MODP). The system is in operational use on the JF-17. The Link-16 MIDS LVT and NDL are two separate networks, possibly being linked by PAF's Erieye and ZDK03 AEW&C.^{xiii}



Fi. 8 - MIDS LVT

(Source: HAVELSAN Inc, Turkey)

The availability of the NDL gives the PAF the flexibility to readily network future airborne assets like the medium-altitude long-endurance (MALE) UAVs. The SDRs used to support Pakistan's indigenous data-links are sourced from overseas from firms such as Harris as well as Rohde and Schawrz.

There are claims of Pakistan having developed its 'own' tactical network & is also progressing in the sphere of SATCOM to ensure BLOS communications capability.

Australia

The Australian Defence Force is developing innovative networked sensortechnologies, and testing autonomous vehicles to offset the smallsize of their forces. They are testing network communications that will permit oneoperator to control a formation of unmanned aerial vehicles that can be programmedto peel off independently for surveillance, or to launch an attack.^{xiv} There are interoperability issues also which have been identified by the Australian Defence Forces (ADF)& measures to overcome them.^{xv}

The ADF plans to use the TULIP system for management of the TDLs - ThroUgh Life Interoperability Planning (TULIP) process. *"TULIP is a structured through project life cycle process. It provides a method to plan for interoperability from the start and continuously assess interoperability. National and platform specifications are used to enhance STANAGs/MIL-STDs for all platforms implementing TDLs. TULIP includes: -*

- *A single TDLs authority*
- *TDL implementation and testing policies*
- *Detailed TDLs standards*
- *Detailed platform specification documents*
- *Integration development testing and feedback processes*
- *Interoperability review, analysis, testing and feedback processes*
- *Supporting tools and configuration management procedures."*^{xvi}

France

The French are progressing a concept of "Guerre Infocentre", or Infocentric Warfare, which emphasizes on the importance of information flows rather than the network itself. The initial program is the Future Air Land Combat Network System, to provide different combat platforms to contribute to cooperative engagement of targets.^{xvii}

Germany

Germany is developing a future soldier system called “Infanterist der Zukunft”, which will introduce new networking methods between combat units and higher command levels. The system includes optical components, soldier-level computing equipment, and a tactical military internet which links voice and data systems.^{xviii}

United Kingdom

The UK has its own Global Information Infrastructure, which is planned as a single, general purpose network, with a specialized security architecture and a family of joint command battlespace management applications. The UK system design will expand to allow multinational forces, such as the United States, Canada, Australia, and New Zealand to also promote collaborative effort to share a common operating picture through Voice Over IP and video teleconferencing.^{xix}

Status of Tactical Data Links in India

"Jointmanship is a key ingredient for success in war. A nation that utilises the combined strength of its Armed Forces effectively will prevail over enemy. We have accepted the strength of this doctrine."

— Air Chief Marshal Tipnis, PVSM, AVSM, VM, ADC, ex- Chief of Air Staff

The above quote resonates with the steps taken over the past two decades to develop the capability of NCO in India.^{xx} With greater focus now on development of niche technologies, Indian forces too, have endeavored in developing system-of-systems which contribute towards fruition of a ‘joint’ effort. NCW lies at the foundation of joint operations. India has understood the gravity of developing NCO or NCW & its utilization across the entire spectrum of conflict. The net-centricity of operations finds mention in the Joint Warfare Doctrine issued in 2017 as well as the Land Warfare Doctrine in 2018. To quote on the aspect of battle space awareness from the Joint Warfare Doctrine for Indian Armed Forces, 2017, listed at page 44,

“32. Reconnaissance and Surveillance of land/maritime/air battle domains will be conducted utilising a broad spectrum of ground, sea, air and spacebased sensors. Inputs of strategic reconnaissance using aerial platforms and satellites will also be made available/exploited. Emphasis is to be placed on timely evaluation and dissemination of intelligence data to the concerned agencies with an intention of shortening the observation to engagement cycle.”

India has to keep pace with the effort being undertaken by some of the leading nations as mentioned earlier, probably ‘at the speed of technology’, if not less.

“[...] in the new strategic environment, Indian forces will be compelled to deter and fight in multiple domains and different theaters. Achieving decisive effects on the ground will not always be India’s main effort—and when it is, such effects can increasingly be delivered from other domains, such as with fighter-bomber aircraft, ship-based missiles, or offensive cyber operations.”^{xxi}

Advances have been made by the tri-services in developing networks which aim towards net-centricity. The succeeding paragraphs list out the communication architecture that has evolved over the past decade.

Navy

The Navy rules the roost when it comes to indigenisation of weapon systems. This drive has resulted in approximately 119 combat platforms & various weapon-sensor suites which has made it a force to reckon with. This has been achieved by the ‘15-year indigenization plan’ covering the period till 2022. The plan has been shared with the Confederation of Indian Industry to garner maximum participation in collaborative ventures. Similarly, a ‘Science & Technology Roadmap – 2025’ is also in place, with a singular aim of developing indigenous technology for naval applications.^{xxii}

In 2019, The Defence Acquisition Council or DAC approved the procurement of the Software Defined Radio (SDR) for the Navy. The radio which holds promise for the future & is in the process of in-scaling is the version developed by the Navy (WESSEE - Weapons Electronics System Engineering Establishment), DRDO & BEL (Bengaluru). The Indian Navy which is already using a ‘data-link’ will serve to benefit from this endeavour. The advantages of the SDR primarily include the capability to work with various waveforms & protocols, easy upgradation & most importantly the aspect of interoperability which is the cornerstone for joint operations.^{xxiii}

As recent as February 2021, the project sanction order for developing SDRs was given to 18 firms under the revamped Defence Acquisition Procedure (DAP) 2020 Make –II category.^{xxiv}

High capacity wireless networks are going to dominate the digital battlefield. SDR based Mobile Adhoc Networks (MANETs) or going to serve the purpose of Combat Net Radios. Spectrum being scarce, there is a need to squeeze in as many bits of information as the selected waveform permits.

These waveforms, available in the upper spectrum of frequency bands identified by the Navy are in the range of (300 to 475+ MHz). Multi-channel modulation will hold the key to make the spectrum resource being shared by a plethora of users at the same time. These waveforms are generally available in the L, S & C bands.^{xxv}

Apart from the Maritime Operation Centres (integrating sea, shore & air assets) established by the Navy, pertinent network related developments in the Navy include the Navy Enterprise Wide Network or NEWN^{xxvi}, Link 11 Mod 1 tactical data link used as well as the Trigun system. All of the above apart from the P8I & IL38SD airborne system which is a force multiplier for the Navy. National Command Control Communication Intelligence (NC3IN)⁶ Network with Information Analysis & Management Centre or IMAC⁷ as the hub has also been established at Gurugram.^{xxvii} NEWN serves as the secure Navy Unified Domain with a linking of all ships & establishments – it is the information backbone or highway which is currently being exploited. The maritime operation centres are linked with that of coast guard as part of the NC3IN providing maritime domain awareness.

Trigun - The Trigun System, as part of the Maritime Domain Awareness Program, has been designed and developed indigenously by the Centre for Artificial Intelligence (AI) and Robotics (CAIR) functioning under the DRDO to enhance battlespace transparency. It has the capability to collect data about the all kinds of civil and military vessel, submarines and aircraft and information being relayed to the information centres or nodes.^{xxviii} Analyzed information is there after shared with submarines and aircraft through satellite communication. The system is in its most advanced stage & by 2024, post integration of AI, will help predict the future response to a developing situation.

The fitment of Trigun (AIS-MDA) has enabled the IL 38SD to undertake Network Centric Operations by improving Battle Space Awareness and informed decision-making. Automated Identification System or AIS data comparison on-board the aircraft helpssanitize the plot and instantaneous data transmission also updates it at the Maritime Operations Centres (MOC) of the Navy.^{xxix}

⁶The Indian Navy has established the NC3IN linking 51 stations, including 20 of the Navy and 31 of the Coast Guard, with a nodal Information Management and Analysis Centre (IMAC). The NC3I links 20 naval and 31 Coast Guard monitoring stations to generate a seamless real-time picture of the nearly 7,500-km long coastline.

⁷The Information Management and Analysis Centre (IMAC) is located in Gurugram. It is the main center of the Indian Navy for coastal surveillance and monitoring. IMAC is the nodal centre of the National Command Control Communications and Intelligence Network (NC3I Network). It is a joint initiative of Indian Navy, Coast Guard and Bharat Electronics Ltd. and functions under the National Security Adviser (NSA).

Link 11 Mod I - For the Indian Navy - Link II Mod I Communication System, establishes Wide Area Network among Naval units (aircraft, ships, submarines, shore establishments, etc) over radio circuits and satellite communications for exchange of tactical data to achieve a COP.^{xxx} There are aspects of interoperability of data during exercises held with friendly foreign countries (FFCs). Case in point of US Link-16 & the Link 11 Mod I used by us which operate as a different set of protocols. Discussions on these interoperability aspects, keeping in mind the availability of real-time data have also taken place between the US & Indian Navy.^{xxxi} Furthermore, The Bharat Electronics Limited or BEL, Bengaluru developed Link 11 Mod I has also been delivered to Boeing as part of the P8I program.^{xxxii} Indian Navy has also signed a Memorandum of Understanding (MoU) with Indian National Centre for Ocean Information Services (INCOIS) for sharing ocean services data, expertise in operational oceanography which will also feature as part of the information being assessed while planning operations.^{xxxiii} The use of GSAT-7 satellite⁸ towards NCW by the Navy is also being progressed with its validation carried out during the TROPEX exercise in 2014. The satlink is also based on the Link 11 Mod 1 waveform as discussed earlier.^{xxxiv}

Airforce

The Airforce had envisaged the development of the Airforce Network (AFNET)^{xxxv} & later the integrated Air Command and Control Systems (IACCS) back in 2008. AFNET was made operational in 2010^{xxxvi} & in 2019, the first node of the IACCS was declared as operational in Bengaluru.^{xxxvii}

AFNET - This is a net which encompasses fibre optics, satellites and multiple other means to ensure that all assets are connected in every station and in every base using Internet Protocol (IP) Multi-Protocol Switching Protocol (MPLS) based Network with Optic Fibre Cables (OFC) as backbone. The network is secured with a host of advanced state-of-the-art encryption technologies & is designed for high reliability with redundancy. IAF also has an exclusive entirely Air Force cellular network, which allows pan India coverage, however, being a CDMA based network, the coverage is

⁸GSAT-7 – Project Rukmini - Positioned at 74 degrees east, GSAT-7 weighs 2650 kg with a payload power of around 2 kilowatts (kW) and a designed mission life of 7- 9 years. Based on ISRO's I-2K bus, GSAT-7 carries payloads operating in the ultrahigh frequency (UHF), S, C and Ku-bands providing a great degree of versatility to relay various types of transmissions. GSAT-7's geosynchronous transfer orbit (GTO) of 249-kilometre perigee, 35,929-kilometre apogee at an inclination of 3.5 degree with respect to the equator allows it to provide a coverage footprint of some 3600 km across IOR.

restricted to near the base only. A material management online system is fully functional & the Aircraft Maintenance Management System is also being integrated, to cater to platforms from Russia, France, UK and the USA. It will finally take the shape of a single EMMS (Electronic maintenance Management System) developed by WIPRO.

IACCS - The IACCS network rides on the AFNET backbone interlinking all assets including air-defence & EW systems. This makes it possible to control aircraft from almost anywhere within the country. There are reports of the operationalization of the Operational Data Link or ODL which will link the pilot's cockpit right to the decision making agency or the sensor-shooter kill chain (SSKC) as it is called. Integration with Navy's Trigun & Army's Air Defence Control & Reporting (AD C&R) is yet to take place, although it has been planned.^{xxxviii} (Refer Fig. 9)

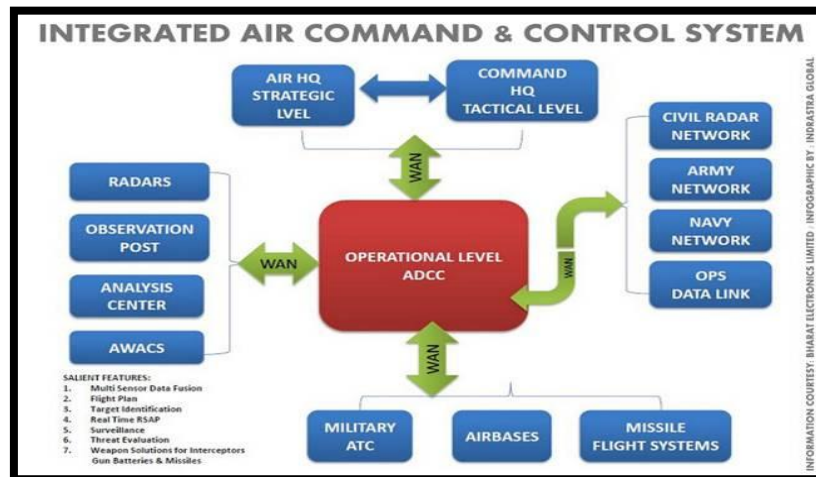


Fig. 9 - IACCS

(Source: AIR DEFENCE IS EVERYWHERE. (2020, July 24). Vifindia.org.
<https://www.vifindia.org/article/2020/july/24/air-defence-is-everywhere>)

The Indian Air Force has already established 5 nodes of the IACCS in the western sector at Barnala (Punjab), Wadsar (Gujarat), Aya Nagar (Delhi), Jodhpur (Rajasthan) and Ambala (Haryana) with assistance from BEL or Bharat Electronics Limited. The 4 new major nodes and 10 new sub-nodes will come up under Phase-II of the IACCS project. While 3 nodes will be deployed in eastern, central and southern India, the fourth is meant for the strategically-located Andaman and Nicobar Islands archipelago in the Bay of Bengal, watching over Malacca Strait.^{xxxix}

Army

The Army is not too far behind & along with the capability development of SDRs as mentioned in the Technology Capability & Roadmap 2018, has taken major steps towards linking of the sensor to shooter to develop a

functional grid. The heart of the system is the Combat Information Distribution & Dissemination System or CIDSS which is in the process of being interacted with the electronic warfare elements, Air-defence network & a Battlefield Management System.^{xi}

For the high speed backbone, the Network for Spectrum (NFS) project has progressed, albeit a bit slow & shall reach completion soon. The NFS has been perceived to be a network based on optical fibre links which offers immense bandwidth to support triple-play services of voice, data & video. All major assets of the Army will be interlinked on this network & last mile connectivity is planned based on Army Static Switched Communication Network or ASCON phase IV^{xli}.

NFS - Network For Spectrum (NFS) has been planned as an Exclusive Optical Fibre based 'Nationwide Communication Network' for Defence Services. This will be a Countrywide Secure, Multi service and Multi-protocol Converged Next Generation Network (NGN) based on exclusive and dedicated Tri-services Optical Transport Backbone.

ASCON - ASCON project will be an upgrade to the existing Asynchronous Transfer Mode Technology to Internet Protocol (IP) / Multi-Protocol Label Switching (MPLS) technology, the ministry said. Optical Fibre Cable (OFC), Microwave Radio, and Satellite will be used for communication, it added. In any operational scenario, the project will provide better survivability, responsiveness, and high bandwidth and enhance the communication coverage of network closer to IB/LC/LAC.

The overarching system of the convergence of the networks of the triad is planned as the Defence Communication Network or DCN^{xlii} which was dedicated to the services in 2016.^{xliii}

Having seen the effort taken for developing the communication architecture, few lacunae still remain viz., training & validation of the joint communication architecture which lends to present a COP as well as interoperability of the systems among the triad. While we are inching towards a DCN, it is JoWIS as hypothesized which holds greater promise towards a seamless network, integrating the various sensor inputs in the tactical battle area or TBA & delivering the optimal package at the point of impact. How JoWIS aims to be an integral & pivotal part of the envisaged 'Mosaic Warfare'⁹ of the future is

⁹Mosaic Warfare -A concept, like the ceramic tiles in mosaics, individual warfighting platforms are put together to make a larger picture, or in this case, a force package. The idea will be to send so many weapon and sensor platforms at the enemy that its forces are overwhelmed.

covered subsequently. Needless to say, that the steps being taken towards achieving a fully functional capable is being noticed by our neighbours too.^{xliv}

How Other Sister Technologies Can Contribute

While we have considered the TDLs used across some foreign nations as well as our own country, it is noteworthy that the future scope in terms of some niche technologies be also brought in this brief. Communication as a domain is extremely dynamic & upwards trend in technology make it an ever-evolving field. Some of the technologies highlighted ahead merit attention as their capabilities can be leveraged for establishing TDLs.

Tactical Cloud

By placing information on the cloud¹⁰, on-demand access to information will be available to all the platforms. Easier said than done, these technologies for a tactical cloud have been under consideration through the program Joint Information Environment (JIE) of the US Forces for over a decade.^{xlv} Main applicability of this cloud is being seen for intra-communication between aerial platforms. JIE would further migrate to Joint Enterprise Defence Infrastructure (JEDI), and specific (Fit-for-Purpose) clouds in coming times. Issues of cyber-security plague the developmental aspects of a tactical cloud, however, it remains a capability to reckon with in the future.

Pseudo-Satellites

Implementing High Altitude Pseudo-satellites or HAPS systems which help in establishing a MANET for the duration of the operation envisaged (Refer Fig 10). HAPS may also be utilised for NLOS communication.

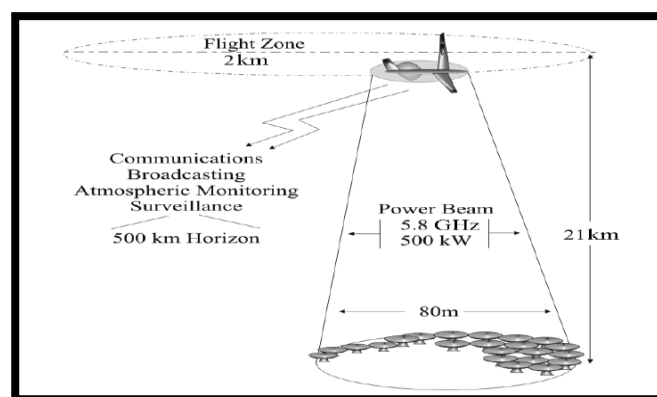


Fig. 10 - SHARP – Stationary High Altitude Relay Platform

(Source: Aragon-Zavala, A., Luiscuevas-Ruiz, J., & Delgado-Pe. (2008). *High-Altitude Platforms for Wireless Communications*. John Wiley & Sons.)

¹⁰“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.” – National Institute of Standards & Technology (NIST) definition, Setember 2011.

Tactical Space Layer

There are also reports of methods being used to fuse data from multiple sensors at multiple altitudes — to include airborne, high altitude and even in space based assets to augment the COP.^{xlvi}

Artificial Intelligence (AI) & Machine Learning (ML)

The use of this technology can only be understated. Avenues of use with respect to use of Alare immense. In the case of TDLs the AI models along with a proper ML engine can help in intelligent spectrum sensing & auto-prioritize the users to send signals or data based on content of the signal message.

These technologies can also be used to make or recommend decisions based on imagery database & suggesting the correct force to counter the threat. Automating the response of the weapon platforms can also be done using advanced programming based on how well the model or engine is trained as per the datasets available.

Technologies such as **Quantum Technology, Private Long Term Evolution (LTE) Networks & HF Communication**¹¹ can also be gainfully used to provide robust data links & complement the existing TDLs.

Way Forward for India – Common Tactical Data Link (JoWIS) & Recommendations

Having seen the triad working on developing or partially developed TDLs, it will be prudent incase steps are taken now to address the issue of interoperability within the systems being tested & developed. It is evident that the backbone network seems to be in place for the country. It is the TDLs that need further deliberation. To arrive at a common denominator in this case will need immense effort & surmounting technological challenges as the systems being used will need to have the form factor or Size Weight & Power (SWaP) considerations based on the platform being employed. Also, issue of LOS & BLOS communication with multiple level of encryption is the need.

¹¹Near Vertical Incidence Skywave (NVIS) - NVIS propagation is particularly useful where radio communications coverage is required in regions where the ground is mountainous or rough because other modes relying on more direct coverage have significant areas where the radio signal is masked or shadowed. When NVIS propagation is being used, the near vertical incident signal is "reflected" by the ionosphere and returned to the Earth over an area of many kilometres either side of the transmitter. In this way good local coverage can be obtained. Frequency of selection is critical & 75 to 80 degrees to horizontal is preferred giving an illuminated area of nearly 350 kilometres.

The software prowess of our nation needs to be tapped alongside the fusion between the academia-military-industry 'iron triangle'. The Navy has clearly taken a lead in this domain of utilizing TDLs. Balance two services may also like to utilize the similar link qualities & protocol to arrive at a 'joint' solution.

Keeping the above in mind, one can list out some of the requirements of JoWIS without getting into the technical details of the exact protocol stack et al.

Hardware Requirements

Software Defined Radios – The sooner we can utilize their potential, the better it is. It is their inherent capabilities to transmit data utilizing various waveforms that makes them the foundation for TDLs.

Interfacing Terminals – Data terminals based on the platform of application need to be tailor-made to meet the SWaP requirements (Ref Fig. 11) of a particular weapon system or static installation. Similar considerations for the antennae will also have to be made.

Communication Backbone – A robust & secure communication backbone which can offer speeds in Gigabits per second is the minimum requirement to have a (near) real-time data flow.



Fig. 11 - Small Form Factor IBM TDL Solution
(Source: IBM Global Services – TDL Solutions)

Information Technology (IT) Infrastructure – The IT infrastructure consisting of switches, multi-data link routers (gateways) & high-speed data processing chips are a pre-requisite for implementing TDLs.

Scalability & Modularity – An important aspect to be kept in mind while developing hardware to make it future-proof.

Software Requirements

Human- Machine Interface or Man Machine Interface (MMI) – Has to be an optimal mix of easy to assimilate & user-friendly dashboards with filters at all levels to prevent a ‘data-tsunami’ at all nodes of operation.

Protocol Development & Communication Technology – Based on the utilization of the RF spectrum (HF/VHF/ UHF) & the waveform chosen, access techniques will have to be designed accordingly. Time Division Multipole Access (TDMA) seems to be the most commonly used scheme so far based on the scarcity of spectrum available obviating use of frequency division architecture. Similarly, protocols will have to be developed, tried & tested before implementation to ensure that all the nodes are able to access the information as intended.

Cyber-Security – As professed by many theorists, the issue plaguing the implementation of NCW lies majorly around cyber-attacks, making the network vulnerable. Encryption algorithms will have to be developed to make the waveforms & data therein un-hackable.

Least Signature in Spectrum – Low Probability of Intercept or LPI signals will be most suited to this requirement, however, a trade-off will have to be considered between the range, power of the signal & jam-resistant properties.

The list above is nowhere exhaustive. Apart from the above, there will be a need to ensure that if a common tactical data link (JoWIS) is what are ultimate aim will be, then the future procurements/ acquisitions/ production should cater to the requirements ab-initio as part of the qualitative requirements specified in Request for Proposal (RFP) documents etc. Methods for backward compatibility or retro-fitment with legacy equipment has to be considered for the risk of not making the existing equipment redundant. One might also like to employ tools such as the Portfolio Theory, Bayesian Analysis or the Monte Carlo Simulations to arrive at logical conclusions while employing JoWIS.

Recommendations

Following recommendations can be suggested for development of JoWIS: -

Recommendation 1. A Program Office for executing the Project JoWIS be set-up with a Joint Oversight Committee (say at HQ Integrated Defence Staff) which will look into the progress made by various cross-functional teams to arrive at developing the JoWIS alongwith implementation in software & hardware.

Recommendation 2. Develop sensor technology which is compatible with the JoWIS envisage d& developed to ensure connectivity when implemented.

Recommendation 3. Implement the fusing of existing networks to include logistics as well as maintenance networks on the same network which can be viewed as a joint picture at the theatre level or later at the National level.

Recommendation 4. More impetus on chip manufacturing. Very small scale integrated circuit design will be of prime importance due to the SWaP considerations.

Recommendation 5. RF Fingerprinting is essential to aid the data links transmit the IFF information. Products being acquired or developed in-house should have this provision during manufacture.

Recommendation 6. Cryptographic advancement is essential to safeguard the implementation & there after implementation of JoWIS. Quantum cryptography, although will make the system complicated than it already is, is the way forward to ensure hack-resistant communication. Similarly, 'Data at Rest' encryption is also essential for data centres or main nodes which will be repositories of information.

Recommendation 7. Exhaustive training will be essential while we implement the JoWIS. This is because a new set of protocols will come into force & the operators will need to be fully confident of the system as well as the new procedures which will come into play.

Recommendation 8. Decision will have to be made to develop in-house systems for such a common data link or utilize off-the-shelf hardware & software as available ex-trade.

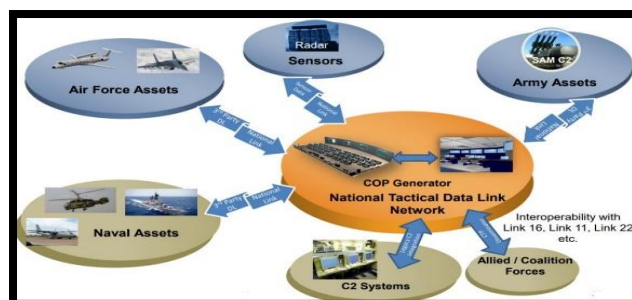
Recommendation 9. Start investing in High Frequency or HF links as with the remaining in-use spectrum already getting congested, might not be suited to meet the overall requirement.

Gestalt

“The four fundamental requirements (capabilities) for conducting network centric operations are Networked Communications, Information Sharing, Advanced Information Technologies such as Agents and Decision Support Algorithms and Networked Enabled Platforms (vehicles, tanks, ships, aircraft and other weapon systems).[...] The military instrument of Network Centric Warfare will have to be forged on suitably integrated organizations, new technologies, joint concepts and doctrines, and joint training and joint communication architecture. Hence the important issues that the Services need to examine in far greater details are:-

- *Jointly evolved communication architecture.*
- *Joint/Integrated organizations.*
- *Joint concepts and a joint doctrine to fight future conflicts.*
- *Induction of new technologies.*
- *Network enabled platforms (tanks, ships, aircraft etc.)”^{xlvii}*

NCW revolves around operations in the cognitive domain & later it is the dominance achieved which translates into an advantage for the side poised with an agile network of networks. To achieve this network, the adoption of a tactical data link, seamlessly integrating the triad is inescapable. It is with a robust data network relying on interoperable tactical waveforms that effect based operations can actually fructify with an overwhelming ascendancy over any adversarial challenge. We are graduating from the IoT to the Internet of Intelligence& it is time we graduated from being ‘network – enabled’ to ‘network-centric’ in this disconnected intermittent & limited bandwidth environment.



CERTIFICATE

The paper is author's individual scholastic articulation. The author certifies that the article is original in content, unpublished and it has not been submitted for publication / web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Disclaimer: Views expressed are of the author and do not necessarily reflect the views of CENJOWS.

Endnotes

- ⁱIndia's Network Centric Warfare Capabilities - Defense Industry. (2019, June 10). Defense Industry. <http://defenseindustry.in/indias-network-centric-warfare-capabilities/#:~:text=In%20the%20Joint%20Doctrine%20of,Theatre%20Battle'%20with%20an%20operati onally>
- ⁱⁱSmith, E. (2002). *Effects Based Operations Applying Network Centric Warfare in Peace, Crisis, and War*", Chapter 2, pp 77-78 http://www.dodccrp.org/files/Smith_EBO.PDF
- ⁱⁱⁱFranz-Stefan Gady. (2020, December 21). *Network-Centric Warfare: Can Europe be ready?* Wavell Room; Wavell Room. <https://wavellroom.com/2020/12/21/network-centric-warfare-europe-defence/>
- ^{iv}TACTICAL DATA LINK – FROM LINK 1 TO LINK 22. (2016). *Scientific Bulletin of Naval Academy*, 19(2). <https://doi.org/10.21279/1454-864x-16-i2-046>
- ^vNPFC - MIL-STD-3011 - Joint Range Extension Application Protocol (JREAP) | Engineering360. (2019). Globalspec.com. <https://standards.globalspec.com/std/13386406/mil-std-3011>
- ^{vi}Miller, John. (2017). JREAP vs Simple. *TDL Technology*, (5), 12–13.
- ^{vii}admin. (2019, February 12). *People's Republic of China's Practice of Network Power* // 中華人民共和國網絡權力實踐 | Red Dragon 1949 / 紅龍1949. Reddragon1949.com. <https://reddragon1949.com/chinese-military-views-peoples-republic-of-chinas-practice-of-network-power>
- ^{viii}admin. (2016, March 16). *Chinese Military Informatization Construction & Development Process* // 中國軍隊信息化建設和發展的過程 | Red Dragon 1949 / 紅龍1949. Reddragon1949.com. <https://reddragon1949.com/chinese-military-views-chinese-military-informatization-construction-development-process>
- ^{ix}admin. (2017, April 25). *中國優先發展網絡戰略信息化戰* // China to give priority to the development of network strategy & information warfare | Red Dragon 1949 / 紅龍1949. Reddragon1949.com. <https://reddragon1949.com/chinese-military-views-china-to-give-priority-to-the-development-of-network-strategy-inform>
- ^xadmin. (2017, March 28). *中國軍事戰雲 ~ Chinese Military Use of the Battle Cloud* | Red Dragon 1949 / 紅龍1949. Reddragon1949.com. <https://reddragon1949.com/chinas-military-infratsructure/chinas-military-organization-intelligence-chinese-military-use-of-the-battle-cloud>
- ^{xi}Costello, J., & McCreynolds, J. (n.d.). *China's Strategic Support Force: A Force for a New Era CHINA STRATEGIC PERSPECTIVES* 13. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf
- ^{xii}Bilal Khan. (2016, March 27). *Pakistan's C4ISR (Part 4): Communications (Data-Links)*. Quwa. <https://quwa.org/2016/03/27/pakistans-c4isr-part-4-communications-data-links/>
- ^{xiii}Bilal Khan. (2015, October 17). *JF-17 Block-2 and Block-3 Details Confirmed*. Quwa. <https://quwa.org/2015/10/17/jf-17-block-2-and-block-3-details-confirmed/>
- ^{xiv}David Fulghum, *Cyber-Hammer*, Aviation Week and Space Technology, May 29, 2006, p.48.
- ^{xv}(2004). Citeseerx.ist.psu.edu. Retrieved May 5, 2021, from <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.174.2663&rep=rep1&type=pdf>
- ^{xvi}ibid

-
- ^{xvii}Giles Ebbutt, *Flaws in the System: Modern Operations Test the Theory of Network Centricity*, Jane's International Defence Review, July 2006, p.61.
- ^{xviii}Staff, "German Soldier Networking System Evolves", International Defense Digest, Jane's International Defense Review, July 2006, p.10.
- ^{xix}Giles Ebbutt, *Flaws in the System: Modern Operations Test the Theory of Network Centricity*, Jane's International Defence Review, July 2006, p.57, 61
- ^{xx}Air Chief Marshal AY Tipnis's message at a seminar held on "Jointmanship under New Technological Environment" at Defence Service Staff College Wellington, March 27-28, 2000.
- ^{xxi}Tarapore, A. (2020). *The Army in Indian Military Strategy: Rethink Doctrine or Risk Irrelevance*. https://carnegieendowment.org/files/Tarapore_Ground_Forces_in_Indian_Military.pdf
- ^{xxii}*The Indian Navy: Trendsetter in Indigenisation*. (2015). Vifindia.org. <https://www.vifindia.org/article/2015/july/28/the-indian-navy-trendsetter-in-indigenisation>
- ^{xxiii}Online, F. (2019, August 20). "Make in India" Software Defined Radio: "Mother" of all solutions for tactical communications of armed forces. The Financial Express; The Financial Express.
- ^{xxiv}Harmeet Singh. (2021, February 20). *Indian Army to get Software Defined Radio (SDR)*. Aviation-Defence-Universe.com; ADU Media. <https://www.aviation-defence-universe.com/indian-army-to-get-software-defined-radio-sdr/>
- ^{xxv}Maj Gen LB Chand. (2020, December 3). *Indian Navy : A Network Centric Force First Off The Block*. Aviation-Defence-Universe.com; ADU Media. <https://www.aviation-defence-universe.com/indian-navy-a-network-centric-force-first-off-the-block/>
- ^{xxvi}*Services / Bay Datacom Solutions*. (2020). Baydatacom.com. <https://www.baydatacom.com/newn.html>
- ^{xxvii}*IT Seminar 2015 at Western Naval Command | Indian Navy*. (2015). Indiannavy.nic.in. <https://www.indiannavy.nic.in/content/it-seminar-2015-western-naval-command>
- ^{xxviii}Mayank Singh. (2020, February 9). *New system with AI to boost maritime security...* The New Indian Express; The New Indian Express. <https://www.newindianexpress.com/thesundaystandard/2020/feb/09/new-system-with-ai-to-boost-maritime-security-2100873.html>
- ^{xxix}Rikeesh Sharma (2013): Transformation of Indian Naval Aviation Post New Inductions, Journal of Defence Studies, Vol-7, Issue-1.pp- 31-48
- ^{xxx}OneIndia Defence Bureau. (2016, February 3). *BEL to showcase gen-next naval systems at IFR*. <https://www.oneindia.com/india/bel-showcase-gen-next-naval-systems-at-ifr-2002208.html>
- ^{xxxi}Online, F. (2019, December 10). *Interoperability of India, US Naval Ships: Tactical Data inter-linking to be discussed at 2+2 Dialogue*. The Financial Express; The Financial Express. <https://www.financialexpress.com/defence/interoperability-of-india-us-naval-ships-tactical-data-inter-linking-to-be-discussed-at-22-dialogue/1790119/>
- ^{xxxi}PTI. (2010, May 12). *Indian-designed Data Link II delivered to Boeing*. The Economic Times; Economic Times. <https://economictimes.indiatimes.com/industry/transportation/airlines/-aviation/indian-designed-data-link-ii-delivered-to-boeing/articleshow/5921211.cms>

-
- ^{xxxiii}V Rishi Kumar. (2020, December 20). *Indian Navy, INCOIS sign MoU to share ocean services data*. @Businessline; The Hindu BusinessLine. <https://www.thehindubusinessline.com/economy/indian-navy-incois-sign-mou-to-share-ocean-services-data/article33378103.ece>
- ^{xxxiv}SauravJha. (2014, September 21). *GSAT-7 bolsters Indian Navy's Network Centric Warfare (NCW) capability*. News18; News18. <https://www.news18.com/blogs/india/saurav-jha/navy-10879-748594.html>
- ^{xxxv}PTI. (2008, August 16). *India developing network centric warfare capability: Naik*. The Economic Times; Economic Times. <https://economictimes.indiatimes.com/india-developing-network-centric-warfare-capability-naik/articleshow/3370673.cms>
- ^{xxxvi}Saurabh Joshi. (2010, September 14). *IAF network goes live | StratPost*. StratPost | India's 1st Defense News Website. <https://stratpost.com/iaf-network-goes-live/>
- ^{xxxvii}*IAF-BEL Launches IACCS To Give Air Defence Control Over Peninsular India*. (2021). Indiandefensenews.in. <http://www.indiandefensenews.in/2019/10/iaf-bel-launches-iaccs-to-give-air.html>
- ^{xxxviii}Saluteindia. (2019, August 20). *MILITARY MODERNISATION: INDIAN AIR FORCE - Saluteindia*. Saluteindia. <https://saluteindia.org/military-modernisation-indian-air-force/>
- ^{xxxix}IndraStra Global. (2015). *ANALYSIS | India's Integrated Air Command & Control System (IACCS) : A NCW Milestone*. IndraStra. <https://doi.org/https://lcn.loc.gov/2015203560>
- ^{xl}*The Official Home Page of the Indian Army*. (2020). Wwww.indianarmy.nic.in. <https://www.indianarmy.nic.in/Site/FormTemplate/frmTemp2PMR7C.aspx?MnId=HmcRMFxtRPYbfmYV1jWRYA=&ParentID=dAbwKLhQ1i3r4w3Agf1PEQ==>
- ^{xli}Fernandes, B. (2020, October 3). *India Army to get new communication network ASCON for Rs 7,796 cr: Defence Ministry*. Republic World; Republic World. <https://www.republicworld.com/india-news/law-and-order/india-army-to-get-new-communication-network-ascon-for-rs-7796-cr.html>
- ^{xlii}*Case Study DCN - HCL Infosystems*. (2016). HCL Infosystems. <https://www.hclinfosystems.in/case-study-dcn/>
- ^{xliii}viralweb. (2016, June 30). *Defence Communication Network (DCN) dedicated to the nation*. Aviation-Defence-Universe.com; ADU Media. <https://www.aviation-defence-universe.com/defence-communication-network-dcn-dedicated-nation/>
- ^{xliv}Muhammad Jawad Hashmi and Sultan Mubariz Khan, "*Emerging Network Centric Warfare Capabilities of Indian Military: Challenges for Pakistan's Security*" - Available as Pakistan National Defence University (NDU), Margalla Papers, Accessed online at https://ndu.edu.pk/issra/issra_pub/articles/margalla-paper/margallapapers2019issueii/04-Emerging-Network.pdf - it brings out how the steps taken towards improving the ISR capability in India would provide it better situational awareness against Pakistan as well as better decision making capability for the commanders.
- ^{xlv}*The "tactical cloud", a key element of the future combat air system | Foundation for Strategic Research*. (2019). FRS. <https://www.frstrategie.org/en/publications/notes/tactical-cloud-key-element-future-combat-air-system-2019>
- ^{xlvi}Strout, N. (2021, May). *Army approves rapid development of Tactical Space Layer*. C4ISRNET; C4ISRNET. https://www.c4isrnet.com/battlefield-tech/space/2021/05/01/army-approves-rapid-development-of-tactical-space-layer/?utm_source=Sailthru&utm_medium=email&utm_campaign=C4ISRNET%205.3&utm_term=Editorial%20-%20Daily%20Brief
- ^{xlvii}*An Operational Perspective of Network Centric Warfare in the Indian Context*. (2021). Usiofindia.org. <https://usiofindia.org/publication/usi-journal/an-operational-perspective-of-network-centric-warfare-in-the-indian-context-2/>

References

1. National Research Council. 2010. *Information Assurance for Network-Centric Naval Forces*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/12609>.
2. Yongbin Wang, Hongbo Liu and Qintao Liu, "Tactical data link based on OMNET++," 2013 15th IEEE International Conference on Communication Technology, 2013, pp. 151-156, doi: 10.1109/ICCT.2013.6820364.
3. Joint Development of Inter- Services Network and C4I2 Systems. (2021). Idsa-India.org. <http://www.idsa-india.org/an-oct-00-9.html>
4. *Tactical Data Link Solutions Certified For US DoD's Secure Internet Protocol Router Network*. (2015). Defenseworld.net. https://www.defenseworld.net/news/12920/Tactical_Data_Link_Solutions_Certified_For_US_DoD_s_Secure_Internet_Protocol_Router_Network#.YluffrUzbVg
5. admin. (2018, October 3). *Chinese Military Analysis of Korean Army Network Centric Warfare Capabilities // 中國軍事韓軍“網絡中心戰”建設現狀及未來發展趨勢 | Red Dragon 1949 / 紅龍 1949*. Reddragon1949.com. <https://reddragon1949.com/chinese-military-views-chinese-military-network-space-forces/chinese-military-analysis-of-korean-army-network-centric-warfare-capabilities>
6. Witvliet, B.A., Alsina-Pagès, R.M. Radio communication via Near Vertical Incidence Skywave propagation: an overview. *TelecommunSyst* **66**, 295–309 (2017). <https://doi.org/10.1007/s11235-017-0287-2>
7. Al-Shehri, S.M., Loskot, P. & Hirsch, M.J. Enabling connectivity for tactical networks in mountainous areas by aerial relays. *TelecommunSyst* **71**, 561–575 (2019). <https://doi.org/10.1007/s11235-018-0532-3>
8. *NVIS: Near Vertical Incidence Skywave*. (2021). Qsl.net. <https://www.qsl.net/wb5ude/nvis/>
9. Spalding, R. (n.d.). *Net-Centric Warfare 2.0: Cloud Computing and the New Age of War*. Retrieved May 1, 2021, from <https://indianstrategicknowledgeonline.com/web/ncw%20cloud%20computing.pdf> - Thesis
10. Akarsu, A. (n.d.). *Overcoming NLoS: Connecting TDL Networks with SATCOM*. Retrieved May 1, 2021, from <https://www.tuyad.org/wp-content/uploads/2018/11/Havelsan-Alper-Akarsu.pdf> - Overcoming NLoS: Connecting TDL Networks with SATCOM
11. MrityunjayMazumdar. (2011). *Defense Media Network*. Defense Media Network. <https://www.defensemianetwork.com/stories/indian-naval-aviation-isr-capabilities-set-for-a-quantum-leap/> - **Indian Naval Aviation: ISR Capabilities Set for a Quantum Leap**
12. Rajesh Uppal. (2021). *Rajesh Uppal / International Defence, Security & Technology*. International Defense Security & Technology Inc. <https://idstch.com/geopolitics/indian-ocean-maritime-security-threats-and-maritime-domain-awareness-mda-technology-requirements/>
13. Sengupta, P. K. (2021, May). *Indian Navy Orders DRDO-Developed & BEL-Made SDRs*. Blogspot.com. <http://trishul-trident.blogspot.com/2021/02/indian-navy-orders-drdo-developed-bel.html>
14. ...: *India Strategic ... Space: Indian Navy eyes 'Gagan' to achieve network centricity*. (2015). Indiastrategic.in. <https://www.indiastrategic.in/topstories549.htm>

APPENDICES
(All Appendices information attributed to synthesys.co.uk)

Appendix 'A'

VARIOUS TACTICAL COMMUNICATION SYSTEM DATA LINKS

NATO Link 1	North Atlantic Treaty Organisation (NATO) Link 1. NATO Link 1 is possibly the oldest Tactical Data Link (TDL) in NATO use. It exchanges air tracks and basic TDL management messages and is used for wide area picture compilation between static sites in Europe. It can also be used to send the air picture to land based units such as Surface to Air Missile (SAM) sites and army C2 units. NATO Link 1 is included in the NATO Air Command and Control System (ACCS). Finally, NATO Link 1 connections now exist with many Partnership for Peace (PfP) nations such as Sweden and Finland for example.
Link 11	Link 11 passes air, surface and subsurface pictures between ground, airborne and maritime units. It was initially intended to provide picture compilation for naval units but has become the most widespread picture compilation TDL, being also found in missile systems such as Phased Array Tracking Radar to Intercept on Target (PATRIOT).
Link 16	The fully developed Joint Tactical Information Distribution System (JTIDS) based TDL, Link 16, passes air, space, surface, subsurface, ground picture, weapons control, C2 messages, Electronic Warfare (EW) information, imagery and TDL management messages between most tactical land, air and naval units. Having a very high degree of security and Electronic Counter Measures (ECM) resistance, it also offers embedded free text and secure voice capabilities. Multifunctional Information Distribution System (MIDS) is a more recent version of the JTIDS bearer system and is compatible with it.
S-Link 16	Satellite Link 16. S-Link 16 messages have been exchanged over SATCOM bearers for many years in order to overcome the LOS limitations of Link 16 Radio Frequency (RF) network. SATCOM allows Link 16 message to be exchanged over thousands of miles.
VMF	Variable Message Format. VMF has been created to provide for the United States (US) Army and Marine Corps requirement for a flexible system providing for Fire Control (FC) and Close Air Support (CAS) operations. VMF systems, unlike most other TDLs, are not bearer dependent. Information may be transferred over various mediums such as UHF, VHF or HF radio, SATCOM or over physical bearers such as copper wire or fibre optics.


Link 22	Link 22 was originally conceived as an upgraded Link 11, its primary aim being to resolve the deficiencies in ECM resistance suffered by Link 11. This new TDL was to be called NATO Improved Link Eleven (NILE). However, the advent of Link 16 demonstrated that Link 11's shortcomings were not restricted to ECM resistance. Link 11 is not, by modern standards, a fast TDL and the more units in a Link 11 net, the slower is the net cycle time. So, to resolve these problems, a new TDL was to be developed which would be called Link 22.
JTIDS/ MIDS	Joint Tactical Information Distribution Systems (JTIDS) / Multifunctional Information Distribution Systems (MIDS), Interim JTIDS Message Specification (IJMS) & Link 16. The JTIDS is a bearer structure which supports two message sets, IJMS and Link 16 J-Series. The two message sets are so closely integrated with the bearer that it is common to consider them as the same thing, so you will normally see them described as JTIDS/IJMS and as JTIDS/Link 16.
ATDL-1	Army Tactical Data Link-1. ATDL-1 is a secure, point-to-point, full duplex data link, utilising serial transmission frame characteristics and standard message formats. The link operates at the basic rate of 1200 bps, with an alternate rate of 600 bps, and also has optional rates of 2400 or 4800 bps.
EPLRS	Enhanced Position Location Reporting System. EPLRS is a secure, jam resistant, computer controlled communications network that distributes near real-time tactical information, generally integrated into radio sets. It is primarily used for data distribution and position location and reporting. It enhances command and control of tactical units by providing commanders with the location of friendly units.
SADL	Situation Awareness Data Link. SADL is installed on US Air Force F-16 and A-10 fighters and coordinates with EPLRS for ground support missions. Additionally, certain other units are able to operate as a gateway between Link 16 and SADL enabling specific exchange of Situational Awareness (SA).

MADL	Multifunction Advanced Data Link. MADL is a future data waveform to provide secure data-linking technology between 5th generation fighter aircraft. It is used by the F-35 to exchange data in close proximity with other F-35 aircraft. Unfortunately, the waveform that MADL utilises is incompatible with that used by the other 5th generation fighters such as the F-22 Raptors Intra Flight Data Link (IFDL).
IFDL	Intra Flight Data Link. Similar to MADL in that it supports the exchange of data and voice for 5th generation fighters but is limited to the F-22 Raptor. IFDL allows a group of F-22 aircraft to exchange information without the fear of detection.
CDL/TC-DL/HIDL	Common Data Link (CDL) / Tactical Common Data Link (TCDL) / High Integrity Data Link (HIDL). In 1991, the US Department of Defense (DoD) designated CDL as its data link standard for imagery and signal intelligence. CDL consists of a secure, jam resistant uplink operating at 200 kbps, and a downlink that can operate at 10.71 Mbps, 45 Mbps, 137 Mbps or 274 Mbps. Currently only the first of these downlink rates is secure.
AIS	Automatic Identification System (AIS). Not technically a TDL, AIS is an automatic tracking system used on ships and by Vessel Traffic Services (VTS) for identifying and locating vessels by electronically exchanging data with other nearby ships, AIS base stations, and satellites.
IBS	Integrated Broadcast System. IBS will replace the current family of UHF satellite intelligence broadcast systems, comprising Theatre Information Broadcast Service (TIBS), Tactical Reconnaissance Intelligence Exchange Service (TRIXS), Near Real-Time Tactical Dissemination System (NRTD) and Tactical Related Applications Broadcast System (TRAP) (which uses the TRAP Data Dissemination System (TDDS) and TADIXS-B broadcast systems). It will receive tactical intelligence information from national and theatre producers, and from tactical Intelligence, Surveillance, and Reconnaissance (ISR) systems, and disseminate tactical intelligence throughout the world via various communications paths (either directly or through a gateway).
ADS-B	Automatic Dependent Surveillance - Broadcast. This is a cooperative surveillance technology in which an aircraft determines its position via satellite navigation and periodically broadcasts it, enabling it to be tracked. The information can be received by air traffic control ground stations as a replacement for secondary radar.
TACFIRE	Tactical Fire Control. TACFIRE was developed as a computer system to conduct fire support operations. The system included central computer systems to analyse and process fire requests, as well as smaller hand-held devices to input messages and transmit over Combat Network Radios (CNRs) to higher echelons.

TACTICAL DATA LINK STANDARDS – NATO FORCES

Demystifying Tactical Data Links

TDL Standards



Digital tactical communications, their associated technologies and their application are as deep and complex as they are diverse. Few, if any, of us understand them in their entirety. This is the second in a series of articles that aims to cast light on the entire range of technologies and applications, providing an insight into some of those areas that we often gloss over.

Following our first article, which introduced digital tactical communication systems, we now become more specific by discussing that class of tactical communications systems referred to as Tactical Data Links (TDLs) and the standards that define them and their operation. These standards define how the TDL works, the structure and content of messages, operating procedures for each TDL and operating procedures for systems using particular TDLs. The technical specification documents are normally North Atlantic Treaty Organization (NATO) Standardisation Agreements (STANAGs) or United States (US) Military Standards (MIL-STDs). TDL STANAGs are in the process of being rebadged as Allied TDL Publications (ATDLPs). The term ATDLP is used in the rest of this article, although some TDL standards have not yet been converted to ATDLPs. Operating procedures are defined in NATO document ATDLP-7.33 and the US Joint Multi-TDL Operating Procedures (JMTOP).

ATDLPs

These documents are intended to “enhance NATO’s operational effectiveness and efficiency” by ensuring that TDLs built for and operated by any NATO force are compatible, interoperable, and interchangeable. In practice despite the best efforts and intentions of the countries involved, it is rare for these aims to be realised.

The documents themselves are not always complete, consistent, and unambiguous. Even when they are, requirements may even be overridden during implementation due to cost limitations or the need to support national industries.

MIL-STDs

MIL-STDs are the United States’ equivalent to NATO ATDLPs. As most TDLs were originally built to US specifications, the MIL-STD is usually the original document. Where NATO has then determined a similar requirement, an ATDLP has been produced. As a general rule, US systems are specified to MIL-STDs, whereas NATO systems are specified to ATDLPs. While both documents are generally alike, there are some differences that may give rise to interoperability issues.

ATDLP-7.33 and US JMTOP

These documents define operational procedures that should be used for each TDL to standardise actions to be taken by TDL operating units and commanders.

For example:

- Establishing and terminating TDL operations.
- Entry into, and exit from, operating TDL structures.
- Altering the structure of an operating TDL.
- Operation of associated voice coordination circuits.

In addition, ATDLP-7.33 provides information about how to plan Multi-TDL networks and other information, such as the level of Implementation of TDL-equipped units and definitions of terms and codewords (including net control codewords) applicable to each TDL.

Standard

In the context of this article, we are referring to technical standards. The technical standard is “an established norm or requirement regarding technical systems. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes and practices.”

The types of technical standards referred to in this article are:

- Standard specification: an explicit set of requirements for an item, material, component, system, or service.
- Standard practice or procedure: a set of instructions for performing operations or functions (e.g. standard operating procedures).

From Wikipedia.

STANAG

In NATO, a STANdardisation AGreement (STANAG) defines processes, procedures, terms, and conditions for common military or technical procedures or equipment between the member countries of the alliance.

Formerly, all the ATDLPs were referred to as STANAGs with their own unique number.

From Wikipedia.

Interoperability

The ability to act together coherently, effectively, and efficiently to achieve Allied tactical, operational and strategic objectives.

From the NATO Glossary of Terms and Definitions (AAP-06 Edition 2018).

Operational Tasking (OPTASK) Link

In addition to the above documents, there is a range of operational documents that either expand on procedures within the ATDLP-7.33 and US JMTOP, define TDL procedures that are system-specific, or that give details of procedures for TDL tasking. Of these, the most significant is the NATO OPTASK Link. The OPTASK Link is a long and detailed NATO message (also used by the US Navy and US Air Force) that covers all TDLs and is published by a commander to task units with TDL operations. It is a set of instructions to all units that are tasked to take part in TDL operations during a particular exercise, operation, or over a stated period of operations. The only problem with the OPTASK Link is that the US Army does not tend to use it - they prefer to use a communications annex to their Operations Orders.

TDL Standards & Responsibility

Within NATO, the organisation responsible for the development, maintenance, and configuration management of NATO Procedural Interoperability Standards (NPIS) for NATO TDL is the TDL Capability Team (CaT). The TDL CaT is a multi-national working group with representatives from NATO nations. The TDL CaT is responsible for the standards shown in the table on the right. *(Latest versions shown.)*

Policy and instructions for tactical data link standardisation and interoperability in the United States are set out in the Chairman of the Joint Chiefs of Staff Instruction (Ref. CJCSI 6610.01E) dated 10 April 2014.

This instruction cites the standards in the table below.

TDL	Associated Publications
Link 4A	MIL-STD-6004
Link 11/11B	MIL-STD-6011
Link 16	MIL-STD-6016 and STANAG 5516 [now ATDLP-5.16]
Link 16 Terminal (MIDS)	STANAG 4175 [now ATDLP-1.75] - no US MIL-STD equivalent
VMF	MIL-STD-6017
IBS CMF	MIL-STD-6018
JREAP	MIL-STD-3011 and STANAG 5518 [now ATDLP-5.18]
Link 22	STANAG 5522 [now ATDLP-5.22] - no US MIL-STD equivalent
TDL Data Forwarding	MIL-STD-6020
MADL	Technical Interface Design Plan / Test Edition (TIDP/TE) in development
CoT	TIDP/TE in development

Standard Title	Publication Number
Interface Control Definition for the International Exchange of MIDS/JTIDS Network (NETMAN T/1)	ATDLP-7.03(A)(1)
NATO Improved Link Eleven (NILE) - Link 22	ATDLP-5.22(B)
Multi-Link Standard Operating Procedures for Tactical Data Systems Employing Link 11, Link 11B, Link 16, IJMS, Link 22 and JREAP	ATDLP-7.33(A)(1)
NATO Bit-Oriented Message (BOM) Tactical Data Exchange - Link 16	ATDLP-5.16(B)
NATO Implementation Codes and Rules (NICR T/1)	ATDLP-7.02(A)(1)
NATO Qualification Levels for Tactical Data Link Personnel	STANAG 5555 Ed 1
NATO TDL Implementation Plan (NTDLP T/1)	NTDLP Rev.3
Standard for Joint Range Extension Application Protocol (JREAP)	ATDLP-5.18(B)
Standard Interface for Multiple Platform Link Evaluation (SIMPLE)	ATDLP-6.02 Edition A
Standard Operating Procedures for Link 1	ATDLP-7.31(A)(1)
Standard Operating Procedures for the Ship-Shore-Ship Buffer (SSSB) and the CRC-SAM Interface - VOL I & II	ATDLP-7.12(A)(1)
Standards for Data Forwarding between Tactical Data Systems	STANAG 5616 Ed 7
Standards for Interface of Data Links 1, 11, and 11B Through a Buffer	ATDLP-6.01 Edition A
Tactical Data Exchange - Link 1 (Point-to-Point)	ATDLP-5.01 Edition A
Tactical Data Exchange - Link 11/11B	ATDLP-5.11(B)
Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & VOL II	ATDLP-1.75 Edition A
xTDL Framework Document [for Representation of TDL in eXtensible Markup Language (XML)]	ATDLP-7.04(A)(1)

From <https://nhqc3s.hq.nato.int> under 'NISPViewer'

CRC = Control & Reporting Centre

SAM = Surface to Air Missile

JTIDS/MIDS = Joint Tactical Information Distribution System/

Multifunctional Information Distribution System

VMF = Variable Message Format

IBS = Integrated Broadcast Service

CMF = Common Message Format

JREAP = Joint Range Extension Application Protocol

MADL = Multifunction Advanced Data Link

TIDP/TE = Technical Interface Design Plan/Test Edition

CoT = Cursor on Target

COMPARISON OF TDLs

	NATO Link 1	Link 11A	Link 11B	JTIDS/MIDS Link 16	MIDS BU2/JTRS Link 16	Link 22	VMF
Major Functions	Air Picture Compilation only Strobe data	Picture Compilation EW Limited C2 Free Text	Picture Compilation EW Limited C2 Free Text	Picture Compilation EW Weapons Coordination & Control Imagery Space Voice and Free Text	Picture Compilation EW Weapons Coordination & Control Imagery Space Voice and Free Text	Picture Compilation EW C2 Free Text Space	Ground Warfare Fire Control CAS Manoeuvre Imagery Free Text
Track Quality	0 – 7	0 – 7	0 – 7	0 – 15	0 – 15	0 – 15	Non defined
Play 'area'	512nm x 512nm	512nm x 512nm	512nm x 512nm	Worldwide (WGS 84)	Worldwide (WGS 84)	Worldwide (WGS 84)	
Positional Granularity	750 Feet	1500 Feet	1500 Feet	32 Feet	32 Feet	32 Feet	Message Dependent
Air Speed Granularity		28dm/h	28dm/h	2dm/h	2dm/h	2dm/h	Message Dependent
Documents	NATO Technical & Message: ATDLP-5.01	US Technical: MIL-STD-188-203 US Message: MIL-STD-6011 NATO Technical & Message: ATDLP-5.11	US Technical: MIL-STD-188-212 US Message: MIL-STD-6011 NATO Technical & Message: ATDLP-5.11	US Technical & Message: MIL-STD-6016 NATO Technical & Message: ATDLP-5.16 Terminal: ATDLP-1.75	US Technical & Message: MIL-STD-6016 NATO Technical & Message: ATDLP-5.16 Terminal: ATDLP-1.75	NATO Technical & Message: ATDLP-5.22	US Message: MIL-STD-6017 NATO Message: STANAG 5519 US Header: MIL-STD-2045-47001 US CNR: MIL-STD-188-220
Examples of Users	NATO ACCS NATO CAOC NATO CRC PFP CRC	NATO Navies and Air Forces Australia UAE Brazil Many others	NATO Ground units Some NATO SSSB sites Other Ground based units	NATO Navies, Air Forces, Ground units Australia S Korea Pakistan Approx. 43 Nations	NATO Navies, Air Forces, Ground units Australia S Korea Pakistan Approx. 43 Nations	Naval Forces from Germany Spain Finland Netherlands Italy Other Nations' Navies	United States United Kingdom Australia Canada Germany Netherlands Other Nations

	NATO Link 1	Link 11A	Link 11B	JTIDS/MIDS Link 16	MIDS BU2/JTRS Link 16	Link 22	VMF
Codename	-	Alligator	Zipcode	Timber	Timber	Elfin	-
Message Type	S-Series	M-Series	M-Series	J-Series	J-Series	F-Series FJ-Series	K-Series
Media	Landline & Microwave	HF & UHF	Landline, Microwave, Radio, Troposcatter	UHF	UHF	HF (Fixed Freq.) UHF (Fixed Freq. and/or Freq. Hopping)	UHF, VHF, HF, SATCOM, Microwave, any other as required
Throughput	1200 or 2400bps	1090bps (1364 with EDAC) 1800bps (2250 with EDAC)	Standard 1200bps. 600, 2400, 4800 and 9600bps also available	STD - 26,880 Packed-2 - 6 words; 53,760bps Packed-4 - 12 words; 107,05 bps	Formatted Code Network Rates: STD - 3 words; 26,880bps Packed-2 - 6 words; 53,760bps Packed-4 - 12 words; 107,052bps ET 0 - 40 words; 358,400bps ET 1 - 61 words; 546,560bps ET 2 - 93 words; 833,280bps ET 3 - 108 words; 967,680bps ET 4 - 123 words; 1,102,080bps	HF Fixed Freq. 1,493 - 4,053bps UHF Fixed Freq. 12,666bps	Determined by bearer
Network Access	Point to Point only	Usually Rollcall (Other methods available)	Point to Point only. Time division	Time Division Multiple Access (TDMA)	TDMA	TDMA (Fixed or Dynamic)	Carrier Sense Multiple Access (CSMA) for systems utilising MIL-STD-188-220
ECM Resistance	X	X	X	✓	✓	✓ (Only when Freq. Hopping Radio used)	✓ (Only when Freq. Hopping Radio used)
Encrypted	X	✓	✓	✓	✓	✓	✓

CERTIFICATE

The paper is author's individual scholastic articulation. The author certifies that the article is original in content, unpublished and it has not been submitted for publication / web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct. The paper does not necessarily represent the views of the CENJOWS.

Disclaimer: Views expressed are of the author and do not necessarily reflect the views of CENJOWS.