

Interoperability is Trained, Not Assumed.

Technology alone cannot deliver readiness. Success relies on the operators, managers, and interface specialists who configure, manage, and secure these systems. NATO's zero-cost TDL Level 2 training, including Model 1 Level 3, delivered at the Integrated Multilink Facility at Geilenkirchen Air Base and Level 3 training, delivered at Uedem, as a joint effort between NATO Allied Air Command Operations Centre TDL Management Branch, the German Air Force Data Link Management Organisation, and CAOC Uedem TDL Section, is therefore essential.

Level 1 provides foundational TDL training, typically conducted at unit level.

Level 2 training prepares Link Operators for tactical employment. It includes system setup, message formats, familiarisation with Link 16 and JREAP, and the use of OPTASK Link. Students gain practical experience with MIDS LVT, MIDS JTRS, SKL, and associated software tools.

Level 3 training qualifies graduates as TDL Managers. It focuses on network design, interoperability planning, and mission-specific configuration. This prepares graduates to manage TDL operations effectively in multi-domain contexts.



These NATO level 2 and level 3 courses are provided without charge to member nations, which helps remove barriers and accelerates readiness. The personal involvement of COM CAOC in the certification ceremony demonstrates the strategic importance of this training. Graduates represent air, land, maritime, and cyber communities.

This training programme provides the Alliance with a shared baseline of competence, a reliable community of practitioners, and a workforce that can support the Digital Backbone. Nations need to know where and how this training occurs because it constitutes the human centre of gravity for future multi-domain interoperability.



Seven crests are displayed: five representing the training providers, with two beneath denoting the Achievement Stage. Together, they deliver manager, operator, and interface-specialist training that turns complex TDL systems into mission-ready interoperability.



1. © Getmilitaryphotos/Shutterstock.com; 2. © ESA-CNES-ARIANESPACE/Optique Vidéo du CSG; 3. © Lockheed Martin; 4. © MCD, Sgt1 Eva Klijn; 5. © US Army, Sgt. Steven Lewis (from left to right)

The Network is the Next High Ground.

NATO's communications networks will evolve into intelligent, self-healing systems supported by artificial intelligence (AI) and quantum-resilient security. AI-based network management will anticipate congestion, compensate for damaged nodes, and adjust frequencies or routing paths without manual intervention. Autonomous mesh networks will connect ground units, ships, aircraft, and space-based assets automatically and will adapt to contested environments.

Quantum-resistant cryptography and quantum key distribution will protect the most sensitive links from future threats. Space-based communication layers, including commercial LEO constellations, will work with military SATCOM to create a flexible network that adjusts to priority traffic in real time.

Follow us on Social Media



© 2026 JAPCC

Disclaimer: This Flyer is a product of the JAPCC. It is produced to provide an update on current topics within the NATO Air & Space Power community. It does not represent the opinions or policies of NATO and reflects independent analysis, opinion, and the position of its author. Releasable to the Public.

This flyer may be reproduced for instruction, reference or analysis under the following conditions: 1. You may not use this work for any commercial purposes, nor may it be used as supporting content for any commercial product or service. 2. You may not alter, transform, or build upon this work. 3. All copies of this work must display the original copyright notice and website address. 4. A complete reference citing the original work must include the organisation, author's name and publication title. 5. Any online reproduction must also provide a link to the JAPCC website www.japcc.org. 6. Panorama Image, top, pp. 2-4: [M] Soldier: © L3Harris; Landscape: © Adobe (Generated with AI); Data Link (left-top): © Copyrighted; Data Link (left-bottom): © X7Teen - stock.adobe.com; Data Link (right-top): © TAW4 - stock.adobe.com; Data Link (right-bottom): © Copyrighted; Cluster: © Copyrighted; Boeing F/A-18E/F 'Super Hornet': © andertan - sketchfab.com, CC Attribution; Carrier: © Usman Zia - sketchfab.com, CC Attribution; HMS Helsingborg K32 Corvette: © Copyrighted - sketchfab.com, CC Attribution; Communications Vehicles: © 42manako - sketchfab.com, CC Attribution; F-35: © shangus930 - sketchfab.com, CC Attribution; Tent: © G4AGamingLabs - sketchfab.com, CC Attribution; MQ-9 Reaper: © Tyler V Howell - sketchfab.com, CC Attribution; C-18A: © Muhammad Mirza Arafi - sketchfab.com, CC Attribution; Thales Ground Master 400 Radar: © flower-3dart/CGTrader, Royalty Free License (no AI); NASAMS: © 3d_mollier International/Free3D, Royalty Free License; Saab GlobalEye: © Saab AB; Helicopter: © Shutterstock AI Generator; AAR: © Bundeswehr/Christian Timmig.

[M] Denotes images digitally manipulated.

Contact: Visit us on www.japcc.org or write us an email at contact@japcc.org.



Connecting the Alliance at Every Level

Taking the Digital High Ground with Multi-Tactical Datalink Integration

Without Connectivity, There is No Multi-Domain Operations.

The rapid emergence of digitally enabled conflicts has forced the Alliance to confront a new reality: modern wars are no longer won by platforms alone. Speed, precision, and resilience of the networks that connect sensors, shooters, and decision-makers in all domains ultimately result in faster targeting cycles.

Events from the India-Pakistan crisis to the Israel-Iran conflict, as well as the war in Ukraine, clearly show that the force with stronger data connectivity gains decision superiority. Tactical Data Links (TDL) have become the nervous system of multinational operations, and they now underpin the situational awareness that political and military leaders rely upon.

This transformation is strategic in nature. Increased defence spending, the European rearmament, and the emerging NATO 'Digital Backbone' require more than modernised platforms. NATO cannot afford 32 separate interpretations of interoperability, as a fragmented

approach creates structural weaknesses in training, readiness, and mission execution.

This is why the forthcoming 'Multi-TDL in MDO: A Success Formula Through Benchmarking' argues for the evolution to a NATO Joint Interoperability Division & Data Link Training Center. It would be the foundation for standards, training, optimisation, and cross-domain architectural development.

'You Can't Shoot What You Can't See and You Can't See Without Tactical Data Links.'

As NATO refines its MDO concept, the message for decision-makers is direct. Victory in future conflict depends on fully networked forces that, synchronised with pertinent civilian actors, operate faster than the enemy can respond. The foundation is a connected Alliance with common standards, shared expertise, and trained professionals. Understanding the problem is the first step. Building the structures and workforce to address it is the essential second step.

F-35: © MCD, SM Christian Schulte, Tunnel Light Effects; © meschi/istockphoto; Code: © Comfisk/istockphoto; Soldier: © Digital/Shutterstock.com; Tunnel: © Air National Guard photo, Senior Master Sgt. Beth Höllner



The Battlespace Has Outgrown Our Legacy Systems.

NATO forces operate today in an integrated and heavily contested environment. This environment includes cyber, space, the electromagnetic spectrum, and all physical domains. It produces unprecedented demands on data flow, survivability, and agility.

However, the Alliance is limited by systems that were not designed for the complexity of modern conflict. Platform-centric networks restrict flexibility. Radio terminals that depend on fixed waveforms and rigid architectures cannot support the speed or volume of information required for multi-domain operations.

The most serious challenge is organisational. Up to 32 different national approaches to TDL Management may result in inconsistent preparation and uncertain interoperability. These inconsistencies introduce operational risk. Poor coordination in TDL employment can slow targeting cycles, reduce situational awareness, and increase the probability of fratricide. In high-tempo operations, this is unacceptable.

Recent conflicts show the importance of rapid adaptation and improvisation. With the transition to a data-centric era, the shift from platform-centric warfare to capability-centric warfare favours the side that connects, synchronises, and exploits information more effectively.

'Interoperability gaps are no longer technical issues – they can become operational risks.'

The Alliance therefore requires interoperable data fabrics that can integrate multiple domains, modern communication tools that outperform legacy stovepipes, standardised training for operators and managers, and a common governance model that ensures consistency.

The central tension is clear. NATO's operating environment has evolved rapidly, yet its approach to connectivity, training, and architectural oversight has not kept pace. Addressing this gap is essential for readiness, deterrence, and credible defence.

Data is the New High Ground.

This section describes the evolution of NATO's TDLs. Link 11 provided the Alliance with its first digital situational awareness, bringing surface ships, aircraft, and command centres into a shared operational picture. In its era, it was a revolutionary system. However, its limitations, including polling-based design, low throughput, and vulnerability to jamming, eventually became clear.

Link 16 addressed these weaknesses. It introduced higher data rates, improved resilience, and time division multiple access. It became the backbone of air operations in the Balkans and Afghanistan. Despite these improvements, Link 16 remained restricted by line-of-sight range and fixed spectrum allocations.

Link 22 expanded beyond-line-of-sight reach and introduced modern cryptography for joint maritime and land applications. Yet it still depended on hardware solutions that restricted its adaptability.

A consistent pattern emerges from this history. Each generation of TDL has been driven by operational

need, but each has been limited by dedicated hardware that cannot evolve at the pace of modern threats.

Software-defined radios (SDRs) provide a broad solution to these problems. SDRs focus their capability in their software, allowing them to host multiple waveforms simultaneously. They can be reconfigured quickly, employ anti-jam measures, and integrate tactical, operational, and commercial networks without replacing terminals.

'Training must include Multi TDL (MTN) and Joint Data Networks (JDN) to be effective.'

Across NATO, SDRs now improve ships by reducing antenna clutter, enabling air forces to reconfigure waveforms during missions, and allowing ground forces to create resilient mesh networks that compensate for terrain. This evolution shows that superiority in the future battlespace will belong to the force that protects, moves, and adapts its data with the greatest speed and confidence.

From Radios to Network Gateways.

The Digital Backbone represents a fundamental shift from platform-oriented communication to integrated, multi-domain connectivity. It provides the structural foundation through which the Alliance can achieve speed, resilience, robustness, and interoperability across all warfare domains.

The solution to increasing technical complexity is not the procurement of additional radios. It is a shift to a data-centric architecture that prioritises interoperability, adaptability, and network resilience. NATO's Digital Backbone represents this shift. It integrates Tactical Data Links, cloud services, artificial intelligence for network management, zero-trust security principles, and the federated structures required for effective mission networking.

SDRs form the centre of this architecture. They provide multi-waveform interoperability and can incorporate Link 16, Link 22, national waveforms, military and commercial SATCOM, and low Earth orbit constellations. They offer rapid adaptability because software

updates replace costly hardware upgrades. Their resilience is enhanced by frequency agility and improved anti-jam features. They scale more easily than conventional terminals and support the growing data demands of multi-domain operations.

'Connectivity only delivers advantage when governance, security, and doctrine evolve with it.'

In this model, communication systems become a set of dynamic services supported by a unified architecture rather than a collection of independent radios. Networks can prioritise sensor-to-shooter traffic, adapt to jamming attempts, integrate new participants quickly, and maintain consistent performance during high-tempo operations.

This architecture requires appropriate governance. Spectrum management, waveform control, cryptographic security, and multinational doctrine must evolve together. Connectivity is an operational effect and should be regarded as such.