Next-Generation Software Defined Radios

Forging the Digital Backbone of the Modern Battlespace

By Petty Officer 2nd Class Chris Parsons, Royal Canadian Navy

Human-machine collaboration visualising multi-domain data to support faster, smarter operational decision-making.

Introduction

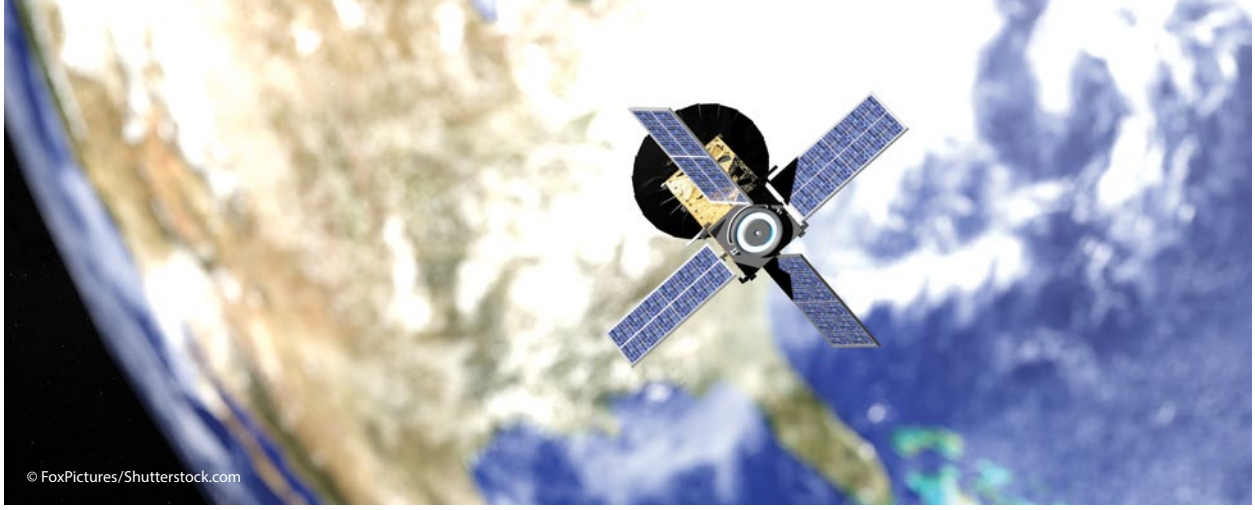
The modern battlespace is no longer confined to the traditional boundaries of Air, Land, or Sea domains. NATO now operates in an integrated battlespace where Space, Cyber, and the electromagnetic spectrum are equally contested. This environment demands a unity of effort that is unattainable without a robust, adaptive, and interoperable communications backbone. In this era, the centre of gravity has shifted from individual platforms to the networks that connect them. Success in multi-domain operations relies on the seamless flow of data, including its confidentiality, integrity, and availability.

As one experienced operator recently observed, 'Multi-Tactical Datalink (TDL) is the bloodstream of multi-domain operations'. Tactical data is not a nicety; it is a strategic necessity. Situational awareness, coordinated fires, and combined defence hinge on assured access to timely, accurate information. NATO nevertheless faces a critical challenge. Its current infrastructure, built on legacy systems and disparate national investments, struggles to keep pace. Maintaining existing TDLs such as Link 16 is no longer sufficient in the face of sophisticated electronic warfare and near-peer adversaries. The Alliance must therefore forge an interconnective digital backbone capable of spanning all domains and adapting to the battlefield in near real time.

The key to this transformation is the Software Defined Radio (SDR). By decoupling waveform capabilities from rigid hardware constraints, SDRs offer the agility, scalability, and interoperability required to bridge the gap between legacy fleets and next-generation networks.

From Link 11 to Link 22: Lessons from the Evolution of NATO TDLs

NATO's experience developing common tactical networks spans decades of both successes and setbacks.



A notional CubeSat in Low Earth Orbit (LEO), representative of small satellite platforms that increasingly leverage modular architectures and SDRs to enable flexible, reconfigurable communications.

The progression from Cold War-era Link 11 to the modern Link 22 illustrates how tactical networking has adapted to evolving operational demands.

Link 11 was innovative for its time. It allowed surface ships, aircraft, and command facilities to exchange digital tracks, delivering a previously unimaginable level of situational awareness. However, its polling topology, vulnerability to jamming, and limited data rates were significant drawbacks. Link 16 addressed these shortcomings by providing higher throughput, improved jamming resistance, and Time Division Multiple Access (TDMA). It became the foundation of Allied air warfare in conflicts such as the Balkans and Afghanistan.

Link 16, however, also has limitations. Its line-of-sight requirement creates coverage gaps over oceans and mountains, while reliance on dedicated terminals and fixed spectrum allocation limits scalability. Link 22 was developed to replace Link 11 and address these issues by providing beyond-line-of-sight connectivity for joint and maritime forces via HF and UHF bearers with modern cryptography. Widespread adoption, however, has been hampered by the cost and logistical complexity of retrofitting legacy platforms with dedicated hardware.

The lesson is clear. Each successive TDL generation is shaped by mission requirements but ultimately constrained by hardware.

As operational theatres expand and data demands grow, NATO can no longer sustain decade-long development cycles for waveform-specific radios and isolated systems. The shift toward SDRs represents the first major departure from this outdated approach.

SDRs: From Radios to Network Gateways

Unlike traditional radios tied to specific hardware and waveforms, SDRs shift core functionality into software. A single SDR can support multiple waveforms, be retuned in real time, and be updated throughout its operational life without costly hardware replacement.

This adaptability makes SDRs the universal interpreters of the battlespace. A single terminal can simultaneously support Link 16, national waveforms, and emerging data transfer capabilities. Software updates replace the need for hardware upgrades, enabling the rapid integration of new operational requirements. Most importantly, SDRs allow NATO commanders to dynamically reconfigure communications architectures by increasing throughput, switching frequencies to avoid jamming, or including coalition partners in mission-specific networks.

SDRs offer significant operational benefits. At sea, they reduce antenna clutter and terminal proliferation on already crowded vessels, increasing task group resilience. Air forces can change waveforms mid-mission, cooperate with coalition partners, or switch to low-probability-of-intercept communications in contested airspace. Land forces can use SDR-driven mesh networks to link units across line-of-sight gaps via unmanned aerial relays and satellite gateways.

In practice, SDRs transform radios from basic transceivers into intelligent network gateways. This allows the convergence of tactical links, strategic satellite communications (SATCOM), and commercial

Over 3,000 engineers and operators participated in CWIX25, NATO's premier digital interoperability event. 'Success depends on the seamless integration of Allied capabilities. CWIX delivers that interoperability', said NATO Supreme Allied Commander Transformation Adm. Pierre Vandier.

networks into a unified system capable of conducting multi-domain operations.

The Space and Commercial Dimension: Satellites as Tactical Enablers

No discussion of future NATO communications is complete without consideration of space and commercial operators. The rise of LEO constellations, such as OneWeb and Starlink, has revolutionised tactical networking. Where military SATCOM was once characterised by limited bandwidth and sparse coverage, LEO constellations provide unprecedented global coverage, redundancy, and bandwidth.

SDRs serve as the interface to this new environment. When configured with appropriate waveforms, they can employ commercial constellations as a secondary transport layer within the military data fabric. For example, a ground unit may employ Link 16 for local situational awareness while using LEO satellites for backhaul to higher headquarters. A naval task group may combine military SATCOM with commercial LEO to build resilience against jamming or interception.

Relying on non-military infrastructure during conflict introduces vulnerabilities but also provides resilience through redundancy. If one network fails, another can assume the load. Integrating SDRs with commercial space assets is therefore a necessity for operating in a contested, multi-domain environment.

Operational Impact: From Case Studies to the Tactical Edge

Recent conflicts demonstrate that communications at the edge can be decisive. The war in Ukraine is a case in point. Ukrainian forces have effectively employed a combination of commercial SATCOM, mobile ad hoc networks, and tactical secure radios to outpace adversaries with less responsive systems. Linking sensors, shooters, and decision-makers in near real time has been critical.

This strategic lesson applies directly at the tactical edge. Consider a ground unit in remote terrain that is unable to contact brigade command because terrain interrupts line-of-sight communications. Without connectivity, situational awareness is lost. With an SDR-enabled mesh network, the unit can route communications through a UAV relay to maintain contact.

Maritime operations in extreme environments, such as the High North or the Baltic Sea, similarly depend on reliable connectivity. Weather and terrain frequently obstruct line-of-sight communications. SDR-enabled Link 22, augmented by HF, SATCOM, and UAV relays, enables seamless maritime situational awareness. For an individual destroyer, this changes operational realities. An un-networked ship is isolated,

Joint Terminal Attack Controllers (JTAC) train with Hand-Held Link 16 (HHL16) devices. Future versions, like the AN/PRC-161 BATS-D, will add SDR capabilities, providing BLOS, datalink-based secure comms, and improved battlespace awareness.

'blind' beyond its own sensors. With SDRs capable of simultaneous communications on Link 16, Link 22, and SATCOM, that same ship becomes a critical node in NATO's Integrated Air and Missile Defence.

Air operations demonstrate similar requirements. In multinational exercises, coordinating dozens of aircraft from various nations is essential. A fighter without a data link is limited to its own radar. When networked into a coalition via SDRs, it can receive targeting data from an airborne early warning (AEW) aircraft, another Allied fighter, or a warship hundreds of kilometres away, extending its survivability and lethality.

Training and Exercises: Building Confidence in Connectivity

Technology alone does not ensure success. It must be tested, validated, and proven through rigorous exercises. NATO values interoperability exercises such as the Coalition Warrior Interoperability Exercise (CWIX), Bold Quest, and Steadfast Defender as proving grounds for SDR-based communications.

CWIX is a key test bed for experimenting with new waveforms, testing SDR configurations, and integrating national systems into the wider NATO network. It treats interoperability as a continuous, iterative process, not a one-time certification.

Seaborne exercises such as Formidable Shield, and air-focused exercises such as Red Flag, demonstrate operational impact. Air, naval, and ground forces from member countries may arrive with different equipment, but depart as integrated, efficient units. This transformation is enabled by accurate SDR configuration. This is how training converts technical capability into the operational confidence on which commanders rely.

Challenges: Security, Governance, and the Human Dimension

While powerful, SDRs are not without challenges. Their programmability is both a strength and a potential vulnerability. Robust cryptography, secure waveform management, and layered cyber security are essential to prevent misuse. NATO must invest in both the radios themselves and the test, certification, and key management infrastructure that underpins them.

Policy challenges also remain. Allies must find ways to share waveforms, intellectual property, and cryptographic solutions without compromising national sovereignty.

Operations centres depend on resilient communications architectures to fuse distributed sensor and platform data into a common operational picture. In many modern constructs, SDRs and tactical data links provide the adaptable transport and standardised exchange mechanisms that make such integration possible.

NATO must also prevent the proliferation of national waveforms from creating new digital stovepipes. These governance issues are central to Alliance unity.

The human factor is equally important. Operators, maintainers, and Joint Interface Control Officers must be trained to exploit the flexibility that SDRs provide. Doctrine and operational concepts must keep pace with technology, or the radios will not be employed to their full potential. Developing personnel is as important as acquiring hardware.

Leadership Roadmap: Building NATO'S Digital Backbone

For NATO commanders, the message is simple. SDRs are more than radios; they are the enablers of the digital backbone for multi-domain operations. A vision-driven roadmap for 2025–2035 must include:

- Standardisation: mandate joint requirements across services and member nations to phase out legacy, single-purpose terminals.
- Governance: establish a NATO Waveform Library to allow secure sharing of approved waveforms across the Alliance.
- Integration: integrate commercial space and terrestrial 5G/LTE infrastructure based on a 'resilience-by-design' policy.
- Doctrine: update doctrine to recognise connectivity as a core mission function rather than a supporting capability.
- Training: invest heavily in simulation and training to ensure commanders and operators understand both the capabilities and the limitations of SDR-enabled networks.

This effort requires political and financial support. Communications programs are often secondary to major platforms such as fighters or frigates. Without connectivity, however, these platforms cannot realise their full operational potential. Leadership must recognise that robust communications are a force multiplier rather than a second-order afterthought. NATO's digital backbone will emerge only through deliberate design, investment, and security planning.

Forward-Looking Vision: 2035–2045 Autonomous, Intelligent, and Quantum-Resilient Networks

By 2035, NATO's multi-domain network must evolve from a collection of interoperable systems into a smart, self-optimising entity. Artificial Intelligence (AI), autonomous network management, and quantum technologies will drive this transformation.

AI-Augmented Network Management

AI-driven controllers will manage network topologies in real time. These networks will predict and address congestion, autonomously route around jammed or destroyed nodes, and assign optimal waveforms to maintain connectivity during attacks.

Autonomous Resilient Mesh Networks

Autonomy will be embedded within the network itself. SDR nodes, from ground vehicles to UAV relays, will autonomously form resilient mesh networks that remain connected in denied environments, reducing cognitive load on operators.

Quantum-Resilient Communications and Cryptography

Quantum technologies will transform security. Quantum-resistant cryptography will protect sensitive NATO communications from future threats, while quantum key distribution could provide unbreakable links. Integrated via SDRs, these technologies will enable secure, real time information exchange across domains and help prevent cyber compromise.

Blending Space and Commercial Assets

The use of LEO, MEO, and GEO constellations will continue to expand. AI will manage traffic across these transport layers (e.g., tactical, commercial, and strategic), dynamically employing the fastest or most secure route for mission-critical data. In contested scenarios, the system will automatically prioritise sensor-to-shooter traffic over routine updates.

Strategic Implications

By 2045, NATO's advantage will depend on network superiority rather than platforms. Network connectivity will maximise the effect of every sensor and weapon system. The Alliance that successfully integrates SDRs, AI, autonomous networking, and quantum-resistant communications will dominate the future battlespace.

Conclusion: The Bloodstream of Multi-Domain Operations

NATO's deterrence and defence credibility will increasingly depend on the resilience of its connective capability. Multi-domain integration is unattainable with rigid, platform-based systems. It requires a dynamic, resilient, and intelligent communications fabric to connect the Air, Land, Maritime, Space, and Cyber domains.

SDRs are the technical enablers for this convergence, and leadership commitment to this solution is essential for the Alliance's success. The digital and tactical networks that support future operations must be safeguarded, expanded, and optimised. NATO must shift its focus from platforms to networks as the primary enabler. In the multi-domain era, network dominance is as important as raw firepower, and next-generation communications are the new backbone of Air, Land, and Sea dominance.

ABOUT THE AUTHOR

Chris Parsons
Petty Officer 2nd Class, Royal Canadian Navy

Petty Officer 2nd Class Chris Parsons, CD, joined the Royal Canadian Navy in 2003 and has served on multiple classes of HMC ships, gaining extensive operational experience at sea. He is currently the Canadian Armed Forces Tactical Data Link (TDL) Curriculum Control Document Manager and has recently served as the Multi-Link Engineering Facility Supervisor. A qualified Joint Interface Control Officer, Chris works with Multi-TDL Networks (MTN) on Canadian Armed Forces platforms, applying hands-on technical expertise to complex integration challenges. His career spans systems integration, multi-link engineering, and Canadian Armed Forces TDL training, supporting personnel readiness and strengthening the operational capability and effectiveness of Canada's tactical data platforms.