M © Ole Andreas Vekve – Royal Norwegian Armed Forces

Redesigning NATO's Targeting Enterprise for Peer Conflict

Digitizing the Kill Chain at the Tactical Edge

By Air Vice-Marshal Mike Hart (ret.)

Introduction and Key Arguments

NATO's targeting enterprise is not fit for purpose. As a legacy of two decades of counterinsurgency (COIN), counterterrorism (CT), and wars against weak nation states, the Alliance lacks the targeting capability required to meet the challenges of a potential war with a peer adversary. It is incapable of handling volumes of data at pace and lacks the capacity to prosecute hundreds of targets per day. It requires a full redesign.

An approach focused on incremental modernization (e.g. by the incorporation of tactical data links) will not suffice. Full digitization, based on cloud computing, dynamic artificial intelligence (AI), and empowering warfighters on 'the Edge' to convert data into targets can provide a robust and versatile platform, increasing capacity more than ten-fold without requiring more human targeteers.

Technology is only part of the answer. To produce a targeting system fit for modern war requires a mindset shift that sees the targeting enterprise as a weapon system, critical to deterrence via enhanced lethality. There are major issues of doctrine and policy that must be addressed, including the relationship of the human to AI in tactical targeting, the balance between centralised and decentralised targeting, the delegation of authorities to expedite kill chains, and the training of a generation of commanders (at all levels), lawyers, and politicians so that they are comfortable with limited, and sometimes no, direct human involvement in the application of lethal force. Putting the right policy framework in place will enable very high-tempo and highly automated decentralised operations at tactical echelons within acceptable risk tolerances, whilst retaining centralised control of strategic targeting where and when appropriate.

There is an urgency to this: redesigning the targeting enterprise is necessary before the exigencies of war reveal the inadequacies of the current system, prevent NATO from exploiting its technological advantage, and in extremis, result in strategic failure.[1]

© Frame Stock Footage/Shutterstock.com

NATO's current targeting enterprise is outdated and unfit for high-tempo conflict against peer adversaries, lacking the speed, scale, and automation required to process and engage hundreds of targets daily.

NATO's Targeting Enterprise: Fit for War?

The genesis of this article was a question from a NATO officer I worked with during Operation Unified Protector (Libya) in 2011. Frustrated by the operation's obsolete technology and 'Post-it note' targeting methods, he proposed that NATO targeting should operate via Tactical Data Link (TDL). TDL would undoubtedly improve the process, but the hard truth is that more is required; indeed, the complexity, tempo and capacity demanded by a major conflict require nothing less than a fully redesigned digitised targeting enterprise, capable of operating at pace, generating and engaging targets from strategic to tactical, from Core to Edge.

In Iraq and Afghanistan, the US and its allies relied on layered and massed intelligence, surveillance, and reconnaissance (ISR) to feed centralised processing, analysis, and distribution facilities, which then produced fused intelligence. Whilst this process could be expeditious, especially for troops in contact, it depended on moving large data volumes from (primarily) airborne sensors, often to different continents for analysis, before intelligence products returned to the operational theatre. This operational model relied on several key assumptions: command of the air (allowing vulnerable ISR aircraft to operate), uncontested access to space, and freedom from effective cyber disruption. Furthermore, facing technologically unsophisticated opponents meant Command and Control (C2) itself was largely invulnerable to kinetic or cyber-attacks. In a future conflict where NATO is unable to easily overmatch its opponent, none of these assumptions will hold true.

In a future major conflict, air, land, maritime, space, cyber, and electromagnetic domains will be intensely contested, with advantage ebbing and flowing across domains and time. Disruption to C2 is inevitable. Units or groups of units may choose to disconnect from the C2 system. Equally they may be forcibly disconnected, either by the physical destruction of headquarters or communications systems and attacks across the electromagnetic spectrum.

To prevail, NATO forces will need to be able to deploy full capabilities toward the front lines, operating in a way that allows cross-domain and multinational operations even when hierarchical C2 is effectively lost.

So long as the ability to securely collect, move, process and exploit data exists on the front lines, technology can enable this, but political and military culture is also critical. Fighting fast in a highly contested environment requires initiative and confidence based on a clear understanding of tactical, operational and strategic intent and the ability to maintain real time understanding of a rapidly changing battlespace. In such an environment a culture of Mission Command with authorities delegated to the lowest appropriate tactical effector could be the difference between success and failure.

NATO's targeting enterprise is currently designed, configured, and resourced to develop and prosecute only a small number of targets per day, typically as single strikes. This limited capacity was starkly evident during Operation Unified Protector in Libya (2011); even against a relatively weak state, NATO struggled to service just 20–30 targets daily, a difficulty stemming significantly from inherent enterprise constraints, not solely from limited aircraft availability. Such performance will be completely inadequate in a high-tempo war against a peer adversary, which will demand the engagement of hundreds of targets daily across all echelons. Key constraints exacerbating this challenge include the limited pool of targeteers (who require mandatory formal training and accreditation), current systems' inability to manage data at the pace required for coherent targeting, and the legal and policy friction inherent in a multinational alliance.

Unlike in COIN and CT, warfare against a state adversary requires an understanding of the enemy as a system of related systems. This perspective will enable NATO to disrupt, degrade, and coerce the adversary through the systematic and sustained application of kinetic and non-kinetic force. Such an approach, in turn, implies equally systematic pre-preparation. Contemporary conflict also demands a targeting system that can seamlessly pivot between deliberate targeting (e.g., pre-planned actions like countering IADS) and dynamic targeting (e.g., immediate responses like suppressing enemy artillery).

Given the volume of potential targets, the overwhelming volume of data available and required, and the need to analyse data at pace, matching targeteers to requirements is not practical without a radical shift in the human/technology balance. To fight effectively, full digitization of NATO's targeting enterprise is essential; its primary intent should be a more than tenfold increase in capacity without expanding the human workforce.

Design Principles

Targeting should be viewed not merely as a process but as a weapons system, whose demonstrable lethality is critical for enhancing deterrence. Effective digitization, therefore, must serve as a demonstrable and significant multiplier of this lethality. Consequently, a digital targeting system itself becomes a key pillar of deterrence, vital for ensuring traditional deterrents are collectively more potent than the sum of their parts.

A digitised NATO targeting enterprise requires the following:

- Survivable ISR from collect to processing, exploitation, and dissemination (PED).
- Strategic to tactical targeting – from critical infrastructure deep inside an adversary state to a single artillery piece on a battlefield.
- Deliberate and dynamic targeting (i.e. both pre-planned and responsive).
- Integrated effects across all domains (e.g. kinetic and non-kinetic such as cyber and electromagnetic warfare).
- Multiple classification inputs from multiple sources.
- Capacity: High data volume and ops tempo enabled by cloud computing and full AI integration.
- Resilience: The ability to function when C2 is disrupted. Capability, capacity, and redundancy from Core to Edge, including the ability for NATO elements to develop and prosecute dynamic targets at the tactical level.
- Tempo: The ability to fight at machine speed. This implies the full use of AI and automation, including automatic data fusion from multiple platforms and sensors across all domains and automated weapon system direction and weapons delivery.

- Interoperability: National (cross-government) particularly to integrate kinetic and non-kinetic action and international (allied). The latter may increase in importance if the US steps back from leading NATO operations as was the case in Libya.
- Adaptability: The ability to quickly integrate new sensors and platforms within a technology stack.

Policy Framework

Targeting is subject to policy and legal controls that, in practice, vary throughout the course and across the spectrum of conflict. In grey zone confrontations, these controls are typically very tight to ensure actions send the correct political signals and minimize the risk of inadvertent escalation. Conversely, during high-tempo, state-versus-state conflict, engagement of some strategic targets will necessarily require tight control to avoid tripping nuclear thresholds. Others, particularly tactical targets such as enemy artillery or missile systems, will require immediate engagement at a speed faster than human decision-making can achieve.

The need for graduated responses drives a dynamic policy approach akin to a 'command rheostat' that determines engagement authorities for different targets and situations. Such adaptations are not controversial; as there are precedents for such control variability as seen in Libya, Iraq, and Syria. What is fundamentally new in a digitised ISR and targeting enterprise is the need to incorporate automation. The system must be configured to support both highly centralised human decision-making, and, when conditions demand, complete autonomy. This includes an AI-based digital system capable of matching weapon to target, providing mensurated coordinates, and directing engagement – potentially without direct human involvement in the decision loop.

This reliance on automation places a premium on the technological assurance of the targeting platform and its diverse data inputs, whether from highly classified traditional ISR, or through rapid, automated analysis and fusion of open-source intelligence, including social media. It will also demand a significant, concerted effort to train the targeteers, lawyers, officials, commanders, and politicians to operate confidently and ethically with systems that involve limited, and in some cases no, direct human control over the application of lethal force.

© anmbph/Shutterstock.com

Display of rocket sections from an intercepted Russian Tochka-U missile in Ukraine.

Technology

A NATO targeting enterprise capable of functioning effectively in a high-tempo conflict, servicing hundreds of targets per day, will demand the capacity to handle vast data volumes at pace. This requires hyperscale cloud computing. For security, this means NATO-operated cloud infrastructure, detached from the public internet, run in Alliance data centres by security-cleared personnel.

The likelihood of electronic and physical disruption, including physical attacks on data centres, C2 nodes, and major intelligence facilities drives an urgent requirement for resilience. Effective combat operations depend on data access; if data resides only on a centralized platform, it becomes extremely vulnerable.

Therefore, the system must be designed with multiple redundancies so that it functions as effectively as possible when attacked. In practice this means enabling units to develop and prosecute targets as close to the tactical Edge as possible. Individual warships, aircraft and land units must be able to continue to collect and use data to target the enemy even when disconnected from NATO or national C2. For instance, in a contested Baltic scenario, diverse multinational assets – such as a Swedish corvette, a Norwegian F-35, and

Finnish land forces – would need to collaboratively share situational awareness and synchronize actions using locally processed data if primary C2 links were severed. This capability requires a distributed cloud architecture, with maximum computing power pushed to tactical levels, enabling disconnected operations for extended periods and re-synchronization with the core when feasible.

Summary

NATO's targeting enterprise is not fit for purpose. It is inadequate to meet the challenges of a large-scale war and is incapable of quickly handling large volumes of data to prosecute hundreds of targets per day. It requires a full redesign.

Technology offers the potential to redesign the NATO targeting enterprise, radically increasing capacity allowing more targets to be prosecuted faster and more accurately. A full redesign, based on cloud computing and dynamic AI, can provide a robust and versatile platform. This approach, which empowers warfighters on 'the Edge' to convert data into targets, could increase capacity more than ten-fold without requiring more human targeteers.

However, technology is only part of the answer. To produce a targeting process fit for modern war requires a mindset shift that sees the targeting enterprise as a weapon system, critical to deterrence via enhancing lethality. With the right policy framework this will enable very high tempo and highly automated decentralised operations at the Edge, within acceptable risk tolerances, whilst retaining centralised control of strategic targeting where and when appropriate.

Addressing these inadequacies is urgent. Failure to act before conflict exposes these flaws would prevent NATO from exploiting its technological edge and could, in extremis, result in strategic failure. ●

1. See Fabian Hoffman: Foreign Policy, 19 May 2025, A Russia – NATO War would look nothing like Ukraine.

ABOUT THE AUTHOR

Mike Hart

By Air Vice-Marshal Mike Hart (ret.)

Air Vice-Marshal (ret.) Mike Hart is Senior Adviser on Defence and Intelligence for Oracle. He spent more than 30 years as an intelligence officer in the Royal Air Force, retiring in 2022. His operational experience encompasses the Middle East, Russia, Africa, the Balkans, and Northern Ireland. Latterly, he worked in key senior appointments in UK Defence Intelligence Operations and ran the UK's cross-government Joint Terrorism Analysis Centre. He worked extensively with allies and is deeply experienced in ISR and targeting. He has wide experience of UK and Allied Intelligence Communities, including Five-Eyes and NATO. Educated at Oxford and Cambridge Universities, he is a Senior Associate Fellow at RUSI and provides geopolitical advice to various think tanks, NGOs and academic bodies.