Heligan
STRATEGIC
ADVISORY

The Digital Targeting Web: The UK's £1bn bet on AI driven warfare

In warfare, tactical superiority – and ultimately the strategic upper hand – hinges on the ability to sense, decide and effect faster than the enemy. Put simply, one's capacity to consistently beat the other side in identifying the enemy on the battlefield, securing authorisation to strike those targets and then executing the resulting strikes, often determines the outcome of conflict. Revered Chinese military general, and author of The Art of War, captured this principle when he wrote – "quickness is the essence of the war."

Much has changed since Sun Tzu's time, but the imperative to think and act quicker than your opponent remains an enduring character of conflict. In modern warfare sensing has evolved far beyond scouts armed with telescopes, now incorporating sophisticated systems such as infrared cameras, satellite imagery and electromagnetic spectrum analysers, all trained on the battlefield and operational 24 hours a day, 7 days a week.

In the decision space, advanced battlefield communication technology supports the real-time transmission of data received by sensors to military commanders across vast distances and AI gets put to work sifting through these data streams, allowing for rapid positive identification of legitimate targets and quick decision making. In turn, precision munitions enable military forces to deliver kinetic effects with heightened accuracy on targets, leveraging advanced GPS guidance systems and hypersonic technology to evade enemy counter measures.

But whilst the technology and systems that exist today will be beyond the wildest imagination of 5th Century BC military strategists – delivering effects at a fraction of the time it would have taken our forebears – they remain fragmented and siloed. The technology has evolved at such a rapid pace that the systems that underpin each segment of the targeting chain remain disconnected, not helped by the dispersion of teams across the battlespace.

This stark battlefield reality, often requiring military planners to revert to mandraulic methods of transferring data from system to system and rudimentary ways to log and visualise this data – often using presentations and spreadsheets – has forced a rethink in the UK MOD. At the top of its priority list is a solution to this inefficiency, a way of connecting each component part of the targeting chain, from sensor to decider to effector – a digital targeting web.

In a nutshell, the digital targeting web (DTW) – referenced fourteen times in the Government's 2025 Strategic Defence Review – will link sensors, decision-makers and weapons systems to speed up how UK forces detect, decide and act on threats. It will provide the British Armed Forces with speed and resilience. The DTW, rather than being a single piece of hardware or software, is conceived as a system of systems providing a digital backbone (or unified data architecture) to the UK Armed Forces' targeting chain, allowing sensors, decision support systems and effectors to plug into it.

Fundamental to the DTW is of course AI. Fed with battlefield data and supported by robust communication networks, it will allow targeting to be carried out in minutes rather than hours, or days. The DTW will in essence wield data as a weapon for the modern warfighter, using AI to enable its exploitation ahead of our enemies.

Timing

The UK faces a formidable challenge in delivering a timely solution, particularly as global conflict intensifies and war technology (or 'war tech') advances at an unprecedented speed. Taking lessons from the Ukraine-Russia conflict, the MOD has instigated the means to procure at speed to ensure the programme maintains momentum. Embeds in the team from CommercialX, the MOD's rapid procurement specialists, is transforming how DTW developers engage with the UK defence SME community, with the hope to bring innovative technology to the table at the pace required.

Current planning aims to have a minimum viable product by November 2026, with the Strategic Defence Review committing to delivery of the DTW in 2027. However, at Heligan we understand this 2027 delivery to be the DTW in 'initial operating capability,' whereby it will be available in its minimum, usefully deployable form. Therefore, we anticipate that 'full operational capability' will not be achieved until at least 2030 – a milestone still nearly half a decade away – at a time when battlespace interconnectivity is accelerating at pace and threats continue to grow.

We anticipate that 'full operational capability' will not be achieved until at least 2030 – a milestone still nearly half a decade away – at a time when battlespace interconnectivity is accelerating at pace and threats continue to grow.

HELIGAN INTELLIGENCE

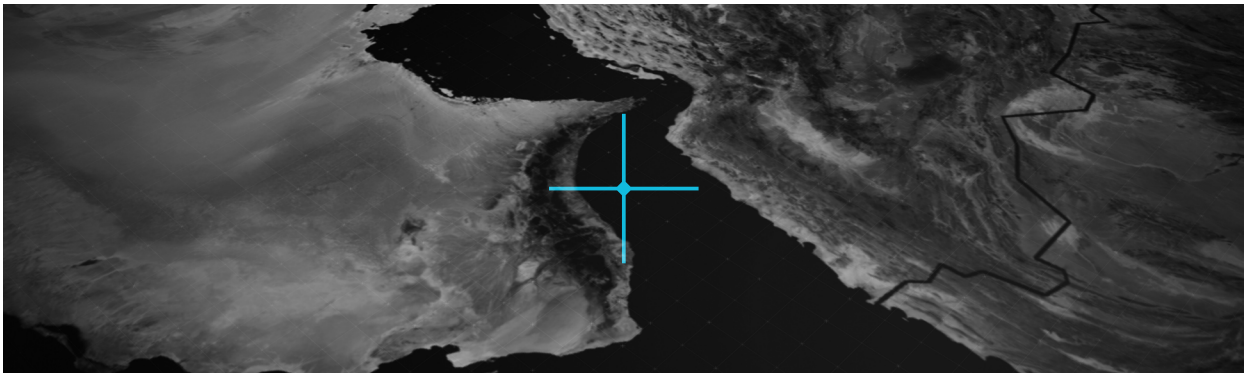
Challenges

Much has been made of the STEM skills shortage across the nation, with trade body ADS recently highlighting in its Quality Jobs Index that there are more than 10,000 annual vacancies across the aerospace, defence and space sectors. This shortage will inevitably affect DTW's effective delivery, potentially limiting project scope and completion timelines. Consequently, its lethality will hinge on the strength of data architecture skills within the UK's SME community and, more broadly, across the national workforce.

By its interconnected nature the DTW will facilitate the transfer of vast amounts of data across the battlespace. This in itself presents significant data security challenges – well recognised in military secure communications environments – requiring 'security by design' to be embedded in the programme from the outset. On top of this, we see challenges in the secure flow of data across security classifications, not to mention integration with allies' systems as we move towards a greater emphasis on multinational allied military operations. In tackling this latter point, we recognise the current use of common NATO architecture and coding in the programme as a positive and necessary step. Therefore, without getting these security and interoperability foundations right, the DTW risks becoming a vulnerability rather than an advantage, undermining operational effectiveness in the very environment it is meant to strengthen.

Additionally, the DTW programme spans multiple government departments including the Military Strategic Headquarters (MSHQ), Defence Science & Technology Laboratory (DSTL), UK Special Forces (UKSF), Defence Digital and the Cyber and Special Operations Command (CSOC), as well as many more. With a vast range of programme stakeholders, the effective coherence of their various requirements will be essential in ensuring the smooth delivery of DTW and its utility across the force. The DTW team's task is further complicated by the government's approach to involve multiple SMEs across the programme, each contributing different elements of the DTW – an approach we support, but one that contains numerous pitfalls if not managed effectively. An effective approach to unifying these stakeholders is therefore vital to prevent fragmentation and the emergence of incompatible system components.

Operationally, as and when DTW goes live, there will inevitably be ethical implications to speeding up the targeting chain and integrating AI into the decision-making process. Chiefly, reducing or removing the human in the loop raises difficult questions about how AI will interpret and apply the Law of Armed Conflict. Another ethical conundrum is accountability – with machines and algorithms taking over much of the cognitive burden in the targeting process, who or what do we hold accountable when targeting goes wrong and civilians are harmed? Despite this, we see AI increasingly being used to support kinetic strike action from the battlefields of Eastern Europe to the theatres of the Middle East. But, in 2026 there are those that oppose the unrestrained reliance on AI – Anthropic has refused to allow its AI to make final kill decisions resulting in it being blacklisted by the US War Department. Therefore, we argue that in lockstep with the DTW's development needs to be the evolution of frameworks for responsibility and oversight to ensure we continue to operate within ethical guidelines and importantly, on the right side of the law.



Final thoughts

The DTW represents the UK's ambitious attempt to regain the decision advantage on the battlefield, albeit at substantial cost. The fusion of sensing, deciding and effecting represents a real step change in how the UK Armed Forces target enemy combatants – a capability that would place it well ahead of any other technologically advanced military. However, previous well-publicised programme failures such as the Ajax armoured fighting vehicle garnered the headlines for the wrong reasons as a result of multi-year delays and critical safety issues. Therefore, it is clear that the task at hand to pull this off, on time and within the £1bn budget is herculean.

But despite the challenges, the Government's embrace of the defence SME community and its novel approach to programme procurement is precisely what the moment demands. If issues of data security, interoperability, stakeholder coherence and ethics can be addressed, the UK stands on the threshold of becoming the first military to realise a fully integrated targeting chain, reinforcing its status as a key shaper of European security alongside France, Germany and Poland.