Modern Targeting in European Militaries

Robert Tollast, Noah Sylvia and Matthew Savill

20 August 2026

Long Read

This paper analyses digital targeting in European militaries, focusing on organisational, procedural and technological integration challenges.

Overview

This paper delivers a critical analysis of modern targeting practices in European militaries, highlighting their transformative impact on operational effectiveness, legal compliance and coalition interoperability in the digital age. By examining both technical and human factors, the paper provides actionable insights for defence and security professionals seeking to navigate the complexities of digital and multi-domain warfare.

Key Recommendations

- **Prioritise organisational and procedural adaptation:** Modern targeting requires not only advanced technology but also changes in processes, culture and delegation of authority to enable rapid, scalable operations.
- **Balance speed with legal and ethical safeguards:** While automation and digitalisation accelerate targeting, robust safeguards must be maintained to ensure compliance with international humanitarian law and mitigate civilian harm.

- **Enhance interoperability among Allies:** Align targeting policies, procedures and systems across coalition partners to reduce friction, prevent redundant strikes and ensure effective joint operations.
- **Invest in human-machine teaming:** Develop clear frameworks for meaningful human control and accountability in automated targeting workflows, addressing legal, ethical and operational frictions.
- **Focus on training and doctrine:** Prepare commanders and operators for the realities of high-intensity, digitally integrated conflict, including the need for decentralised decision-making and risk management.

This paper is essential reading for defence sector leaders, policymakers and practitioners aiming to modernise targeting capabilities and ensure operational success in future conflicts.

Introduction

On 28 February 2026, the US and Israel launched a massive strike operation against Iran. The US's Operation *Epic Fury* carried out strikes at a sustained tempo not seen since **the invasion of Iraq in 2003**, with some reports claiming that nearly **900 strikes** were carried out in the first 12 hours. This scale of targeting was only possible through the collation and cohering of decades of data points from a myriad of sources that both enabled hundreds of strikes in a matter of hours and facilitated hundreds of daily strikes for the following five weeks.

The scale and tempo of the strikes demonstrate the centrality of targeting to modern operations, continuing a trend that has been seen in Ukraine and recent Israeli operations in Gaza, Lebanon, Syria, Iran and Yemen. Various countries, **including the UK**, have made an increase in their targeting capabilities core to their force modernisation and enhancement initiatives, with one European general describing their desire to identify **3,000 targets per day**.

Much of the public attention focuses on the technical means of enabling such capabilities, especially the **methods and platforms** that integrate the disparate data streams into targeteers' workflows. For example, the Israelis use **systems that 'bank' targets** ahead of a conflict, with AI-enabled databases tracking and updating thousands of targets, while the US famously uses Palantir's **Maven Smart System** to host, manage and even automate their targeting workflows. This approach to modern targeting envisages a deep integration of intelligence collection and strike systems across a joint force, such as the **US Combined Joint All-Domain Command and Control** concept. The connection of **any sensor, any decider and any effector** seamlessly across all domains remains more a guiding vision than an operational reality, despite significant developments in multi-domain integration in **Ukraine** and the **Iran war**.

Far less attention has been given to the organisational, procedural and human elements of modern targeting, despite the changes in processes, procedures and organisational culture required by the adoption of large-scale, digitalised integration enablers. This paper seeks to fill this gap, describing modern targeting while detailing its non-technical considerations for both policymakers and practitioners. It is bounded by a focus on European capability, especially UK capability, and aims to inform human, policy and procedural considerations around the implementation of the UK's **Digital Targeting Web** (DTW).

The paper begins with a description of targeting grounded in traditional doctrine, then outlines what targeting comprises from policy, procedural and operational perspectives. The second section illustrates the operational challenges presented in high intensity, near-future conflict between British and Russian forces, especially in sensing, finding and prioritising targets if the joint force is digitally integrated. The third section frames the frictions – both theoretical and observed – in modern targeting, especially those arising from decision compression and automation.

+ Methodology

+ What is the DTW?

What is Targeting?

Targeting, as commonly used **in the media** or by the layperson, is usually conceived as the final act in the use of force, such as when a building or an individual is said to be 'targeted' by an airstrike. The use of such equipment as 'targeting pods' of the type often found on aircraft, containing the sensors necessary to precisely guide a weapon to its 'target' – the individual or location being struck – gives extra weight to the idea of targeting as a primarily battlefield activity. Yet, in both language and practice, targeting is broader than this and begins ahead of the use of force or activity: it is as much a concept or a process as an activity on the battlefield, and its application sits at the heart of the successful use of military force.

In **UK military doctrine**, targeting is described as 'the command process that identifies, selects and prioritises targets, in order to direct action to achieve required outcomes'. **For the US**, targeting is 'the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities'. **NATO's definition** states that targeting 'involves the process of selecting and prioritising targets … and matching the appropriate response to them, taking account of operational requirements and capabilities, with a view to creating desired effects in accordance with the commander's objectives'. In simpler terms, targeting is the process by which the effects necessary to achieve military goals are identified, and military capabilities are matched against targets to achieve those effects. In

many cases, those might be strike capabilities – where the activity is to launch or fire a projectile of some sort, using physical violence to achieve an effect. However, targeting might just as plausibly use information operations (to influence morale or a target population's attitude) or cyber capabilities or electronic warfare (to blind an adversary or undermine their communications).

Components of Targeting

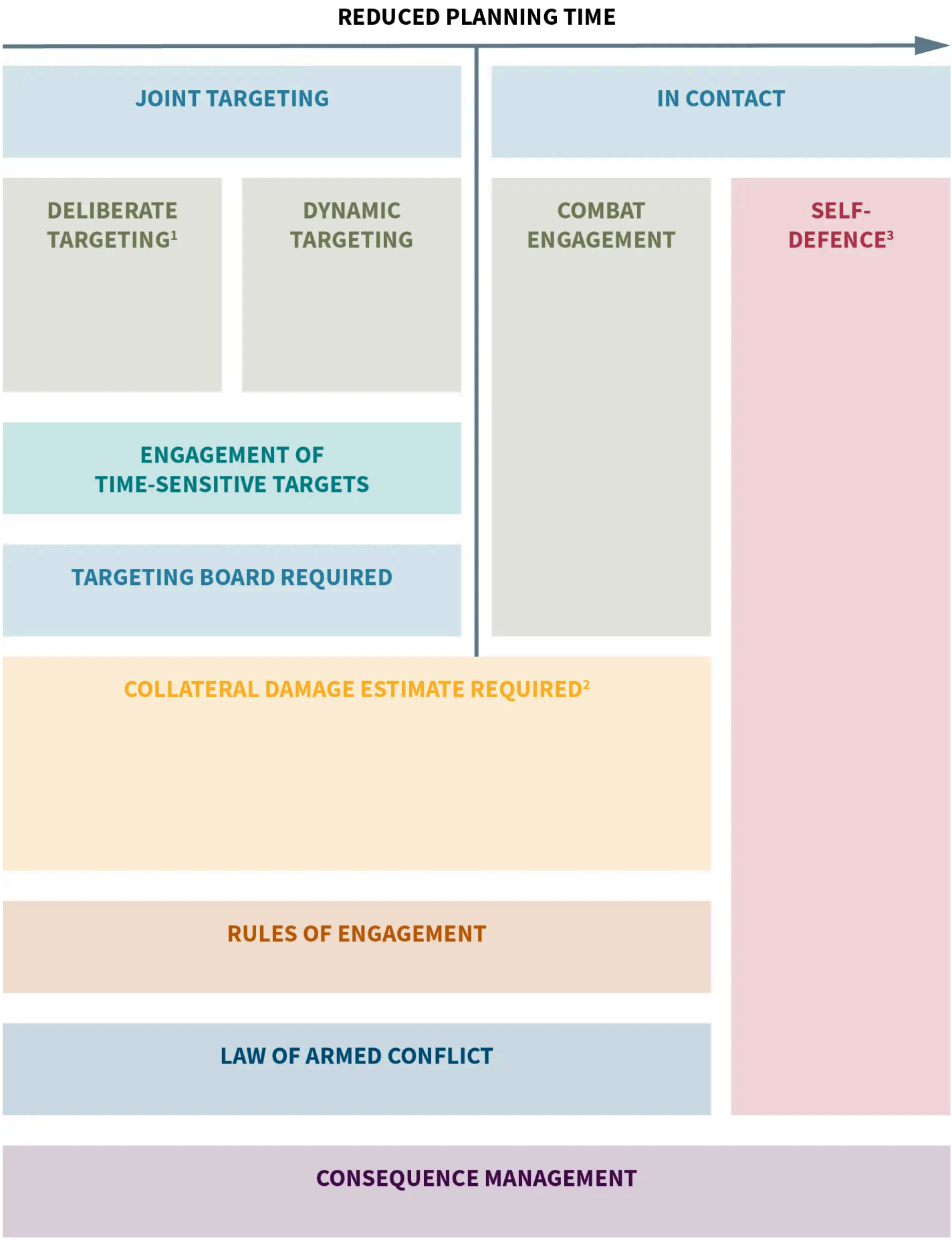
Targeting has a number of requirements or components. For inputs, it requires goals, expressed as an overarching policy, mission and objectives. From these, targeteers can deduce effects to be achieved. Targeting needs information, potentially in vast volumes, either from secret intelligence or open sources. This information will vary, from video and images and electronic emissions to geography, weather, opinion and social analysis. This is particularly the case when it comes to 'full spectrum targeting', where non-violent means of achieving influence are involved. '**Target Systems Analysis**' – the process of analysing adversaries and audiences for influence – draws upon this data to run the process of matching capabilities to targets and desired effects. Critically, targeting needs not only information on the adversary, but also a comprehensive picture of one's own forces and capabilities; no goals will be achieved if targeting sets out to apply non-existent capabilities to a problem, or wildly over-stretches limited resources. On the battlefield, this situational awareness is needed to deconflict activity and to prevent harming one's own forces ('fratricide' or 'blue-on-blue').

Targeting also needs a framework within which to operate, including legal and policy direction. International Humanitarian Law (IHL, also called the **Law of Armed Conflict** (LOAC), governs the use of force in conflict, but this is insufficient on its own for a number of reasons. First, operations might be conducted outside war, and targeteers therefore need more detail on who or what can legally be the subject of targeting, whether that might be locations,

capabilities, groups or individuals. This is supplemented by policy direction on any additional freedoms or constraints, for example, sensitive sites protected from targeting. Finally, the conditions under which capabilities can be used, or force unleashed, need to be set out.

These requirements result in a series of rules, guidelines and directions, codified as a collection of documents. In the UK, a **Targeting and Effects Directive** will define who or what are defined as the targets, and provide guidance on the conduct of targeting, as well as who can take what decisions. **Rules of Engagement** confirm the circumstances under which military forces may operate and use these capabilities. Guidance will be given on the question of civilian casualties ('collateral damage') and at what point in the planning process approval can be given for operations where there is a risk of civilian casualties. Militaries can never deliberately target civilians with lethal force if they wish to remain compliant with IHL, but this does not mean that civilians cannot be killed or injured as a consequence of military action: rather, the risk must be quantified, mitigated and then accepted by someone authorised to do so as part of the decision-making process. A list, database or other type of system will provide more detail on priority targets and the preferred means of affecting them, as well as targets which have some restrictions or which are not to be struck (leading to such concepts as the '**Restricted Target List' and 'No Strike List**').

Figure 1: The Engagement Continuum in an Armed Conflict Situation


REDUCED PLANNING TIME
JOINT TARGETING
IN CONTACT
DELIBERATE TARGETING[1]
DYNAMIC TARGETING
COMBAT ENGAGEMENT
SELF-DEFENCE[3]
ENGAGEMENT OF TIME-SENSITIVE TARGETS
TARGETING BOARD REQUIRED
COLLATERAL DAMAGE ESTIMATE REQUIRED[2]
RULES OF ENGAGEMENT
LAW OF ARMED CONFLICT
CONSEQUENCE MANAGEMENT

Notes:

1. Deliberate targeting includes scheduled and on-call targets.
2. Collateral Damage Estimation (CDE) for joint targeting will be as specified in the operation plan (OPLAN) Annex II – Targeting. Combat engagement is not a joint targeting activity that uses the formal CDE process. In a combat engagement, the on-scene commander will conduct a basic, non-written collateral damage estimate (in accordance with CICSI 3160.01), using their best judgement, adhering to IHL/LOAC principles and taking all feasible precautions to minimize collateral damage, given the situation at the time.
3. In accordance with national laws and policy, using the principles of Necessity and Proportionality. It is generally accepted within NATO that self-defence encompasses the use of necessary and proportional force, including deadly force, to defend against an attack or imminent attack.

Credit / Source: NATO, 'Allied Joint Doctrine for Joint Targeting', AJP-3.9, Edition B, Version 1, November 2021, p. 35, <https://assets.publishing.service.gov.uk/media/618e7da28fa8f5037ffaa03f/AJP-3.9_EDB_V1_E.pdf>, accessed 7 January 2026.

There are also different **categories of targeting**, mostly characterised by the extent to which they are planned well in advance, or emerge during operations. These categories are shown in Figure 1. Deliberate Targeting is where the target is identified and located during the planning process, often days or even weeks in advance, and therefore the activity against it has received the most extensive level of preparation. This is often the case where the target is large, sensitive or complex. By contrast, Dynamic Targeting takes place against targets which might best be called 'targets of opportunity'. They may have been identified, but not located, during the planning process, or they may have received limited attention and emerged during other operations, or within 24 hours of the activity being launched. Across both types of targeting will be Time-Sensitive Targets – those that exist with only limited windows of opportunity, and which therefore require prioritisation for activity, or the acceptance of more risk.

Targeting does not end when the target has been struck or operations conducted, because the impact of the operation has to be evaluated to determine whether the operation was successful (in which case, the desired effect has been achieved or new opportunities might emerge) or unsuccessful (in which case, a repeat operation may be required or a new approach tried). The cumulative impact of tactical activity must be analysed to either validate or

challenge the Target Systems Analysis which produced the original recommendations for prioritisation, capability choices and risk. Targeting is therefore a cycle, with many iterations, which extends from the top levels of government down to the operator on the battlefield.

The Targeting Cycle

Targeting as a process tends to operate in cycles, because of the importance of measuring the impact of operations as feedback for future planning. If the desired impact has not been achieved, fresh attempts will have to be made, but it makes little sense to do so in the same manner if it turns out the methods employed were ineffective. Conversely, success may make a new or coordinated set of operations easier, change targets and their significance, or even obviate the need for more operations against similar targets. In any case, there are multiple cycles taking place at three different levels:

- the major decisions on policy and direction being taken at the strategic level (that is, within government and relating to the purpose of the war or campaign);
- the translation of that guidance into the plans and allocation of forces (usually the operational level);
- the detailed planning of missions and execution of the activity (tactical activity).

The second of these is generally called **Joint Targeting** while the strike or operational activity itself falls under execution.

The Joint Targeting process describing the steps from initial direction through to post-action assessment generally has around six phases, as shown in Figure 2.

Figure 2: The Joint Targeting Process

Credit / Source: The authors, created with assistance from ChatGPT.

Execution of steps within this, especially of dynamic targeting, has been described in a number of ways, often trying to add new letters or numbers to an already clunky acronym: from the 'War on Terror's' F3EA (**Find, Fix, Finish, Exploit, Analyse**) to the more recent F2T2EA (**Find, Fix, Track, Target, Engage and**

Assess). The principles and components, however, are very similar: intelligence and information must be collected and analysed, and targets must be located and then tracked or surveilled and monitored. The detail of what capabilities, at what time, and for what duration, must be determined; then, the activity can be conducted. Finally, the results must be observed, understood, reported and analysed.

Requirements for Targeting

Targeting in all senses – concept, process and activity – places considerable demands on modern militaries if it is to be done well. First, it requires networks, both institutional and communicative. Targeting is fundamentally about the ability to process and move information around, ideally as rapidly as possible, but also with high degrees of reliability and security. This has implications for the processing capability and capacity of any digital components of the system, as well as the human elements, who must balance making supporting decisions quickly with being prepared to face close scrutiny, especially in cases where lethal force is being used.

The second requirement centres around capacity and the processes and systems that support it. Along with speed, capacity is increasingly a challenge, especially in industrial warfare. Targets might number in the hundreds per day, as opposed to counter-terrorism operations which might result in planned operations once every few weeks, and more dynamic targeting several times a day. To facilitate this, processes must be flexible. One of the most important concepts in targeting is that of authority, combined with delegation: who can take what decisions. This reinforces the idea of targeting involving a network, because while many decisions can be delegated, some decisions on very sensitive targets cannot be delegated because they are made at the very top of government by ministers and senior officials. What is described above as a tactical process on a particular activity must therefore be supported by resilient

connectivity that can stretch from the top of a defence ministry to a combat platform operating on the front line.

Third, countries must have appropriate technology. The information gathered must be protected, involving security through classification and digital encryption, which can be partially offset by maximising temporal relevance. But in modern operations, where maximum benefit comes from coordinating and synchronising activity, this network must not only reach vertically through government but also stretch horizontally across force and environmental boundaries. Interoperability or compatibility is an essential component of not only these systems, but also processes and culture, because cyber operations, electronic warfare and strike capabilities might all need to be synchronised to affect complex or well-defended targets. Practically, land, sea and air forces will need to coordinate with space-based capabilities and special forces, including with international partners.

Finally, a country or coalition must have the C2 systems and structures to synchronise the targeting effort effectively and provide the best levels of oversight and delegation. That necessitates a culture where risk tolerance can be set and modified, and where policy and legal constraints can be both articulated and varied throughout an operation.

Targeting can be conducted on a mostly tactical basis or within component boundaries, largely under normal rules of engagement as what is called **Combat Engagement**. But the tools available to modern militaries, adversary defensive capabilities, and the volume of information available all offer challenges or opportunities for exploitation to the side which can distinguish important information from sheer volume and (increasingly) target not just with precision, but at a larger scale.

This section described the processes in targeting which aim to match the campaign commander's intent and war aims (including political

considerations) with various capabilities, including different types of weapons and non-lethal actions, and the cyclical iterations of these processes. The second section aims to illustrate aspects of these cycles in a large-scale combat operation, to understand tactical and strategic problems which may arise when trying to massively accelerate or automate targeting.

Targeting Challenges in Large-Scale Combat Operations

Due to the changeable character of conflict, the following section seeks only to describe targeting scale and complexity, rather than the probable course of a campaign. It is not exhaustive, and does not include, for example, intelligence collection capabilities of various crewed aircraft or communications intelligence that can be intercepted in various ways by airborne platforms.

Taking the UK's Chief of the General Staff's ambition of a **brigade defeating a Russian Combined Arms Army** (CAA), it is worth considering the vast targeting picture of this numerically superior adversary across the **battlefield geographic framework.** One can then examine aspects of deliberate and dynamic targeting, and the problems facing targeteers, planners and supporting intelligence analysts.

Under time pressure, targeting staff at every level and in different branches of the joint force must identify priority targets, which are matched with the appropriate effect. This is meant to overwhelm the enemy target system in a way that supports the component commander's intent and the joint forces commander's strategy, while limiting civilian harm. As previously described, the sheer number of potential targets that must be identified with existing capabilities could place unprecedented strain on targeting staff and the intelligence staff who support targeting. It is useful, therefore, to query the extent that automated targeting workflows might aid targeteers in such a crisis.

Development and Prioritisation

Consider the raw data from ISR assets presented by a CAA, supporting phase two of the cycle, target development and prioritisation (see Figure 2). Combining these layers of data generates a complex and moving targeting picture across thousands of square kilometres for higher headquarters, potentially encompassing thousands of target entities.Some of these may be co-located with civilians or close to friendly forces, as the campaign progresses.In many instances, this may not be apparent, as far-flung units limit radio emissions and other indications of their location.

Rapidly accessing and clearly visualising targeting data layer-by-layer as it changes dynamically informs subsequent intelligence preparation of the battlefield. **Doctrinally**, this preparation is described as closely linked to the targeting cycle. There is an understandable attraction to automating some of these collection and surveillance processes in a large-scale combat operation – for example, deciding where to send uncrewed system X or Y based on automatically identified asset availability. However, enemy forces can be expected to adapt and introduce as much inefficiency into targeting as possible.

The following examples introduce problems which could fundamentally change how our forces fight. Currently, NATO corps and divisions focus targeting on the deep battle, which broadly encompasses enemy higher headquarters, logistics nodes and long-range threats. Brigades fight forces in the 'close', where manoeuvre units are in almost continual contact. Recent discourse, spurred by **developments in Ukraine**, has revealed tensions over traditional targeting priorities between command levels across the geographic framework, because lower-level reconnaissance and strike capability is rising at range. These tensions are not new (see the 2021 **Integrated Operating Concept**) but debates over the deep–close–rear framework will probably continue as

reconnaissance and strike capabilities expand, particularly from DTW programmes.

The following sections explore the tensions this could present to higher level planning and synchronisation of operations.

Finding Targets in the Electromagnetic Spectrum (EMS)

Once a campaign begins, enemy forces will invariably move and seek cover. Because of this, one stated aim of the UK's DTW initiative increases the focus on dynamic targeting. It **acknowledges that** UK commanders 'require targets to be quickly identified and struck using data from satellites, drones, EW systems, soldiers on the ground and other domains both sovereign and allied'. The DTW aims to multiply dynamic target strikes by turning the joint force into a networked reconnaissance and strike system.

Intelligence fusion efforts from Ukraine have found that **signals intelligence** is critical for rapidly locating moving target entities, due to satellite ISR latency. In the EMS alone, intelligence support for the targeting process is extraordinarily complex. For example, the Russian 6th CAA's recent organisation incorporates **170 drone crews** attempting to deny enemy manoeuvre and resupply, striking directly or directing fires. Some of these drones may have short range (10 km) and carry 30 mm grenades, while others may be fixed wing and enable ballistic missile strikes over distances of 100 km, so identifying their ground station signals is critical for targeting prioritisation.

For British brigades fighting in the close(yet currently receiving EMS intelligence analysis largely from **division**),the EW picture presents several challenges. Direction-finding equipment can detect, find and classify dozens of signal sources at once depending on terrain. This SIGINT (signals intelligence) task also assists in locating high value targets, particularly mobile frequency emitters such as **air defence systems** and specialist EW systems. Certain truck-

mounted jammers, for example, could be co-located with targets such as headquarters.

Mapping the electronic order of battle includes analysis of radio frequencies, which could **identify units;**[1] for example, some Russian headquarters are equipped with **satellite communication** systems operating in the S-band frequency range. This may result in further reconnaissance assets being tasked. If identified as a headquarters, this target can then be added to the **high payoff target list**, managed by the Joint Targeting Coordination Board, a staff organisation that **coordinates targeting** across domains through the campaign. Such a high payoff target may be electronically attacked –for example, to suppress it if it is located near civilians – or struck with explosive weapons. If located in a built-up area, careful consideration may be required if forces are to remain compliant with LOAC.

For the EMS targeting picture at depth, a CAA **at full strength** will have two mechanised and one armoured division headquarters. For sustainment, a CAA will have a logistics brigade, as well as railway logistics and engineering units, all producing signals multiple times per day. In headquarters alone, these represent at least another 40 to 45 potential targets, assuming additional fall-back headquarters.

Rapidly prioritising targets across the battlespace at depth must consider layered air defence, in the form of air defence regiments in the brigade: from manoeuvre element defence – short-range systems like Strela-10 and Pantsir – to dozens or even scores of medium-range systems in the CAA. Associated radars will need to be rapidly identified when they emit and can operate in different modes for '**surveillance, targeting or defence**'. Systems such as the **S-400 Triumf** not only produce identifiable radar signals but also have **C2 nodes** for each battery, battalion and regiment. While these signals can be rapidly

analysed in the **air domain**, intelligence fusion will be required for joint suppression and destruction of enemy air defences.

There are further challenges to rapid target location in the EMS. As enemy elements manoeuvre, ground surveillance radars can provide another reconnaissance layer for targeting, by identifying vehicles and people moving on foot dozens of kilometres away. Still, visual identification will be critical. Ground surveillance can detect scores of targets – potentially hundreds – depending on terrain. Counter-battery radars, meanwhile, enable the detection of scores of enemy guns at considerable range but fall short of detecting some multiple-launch rocket systems at their maximum range.In the wide-open spaces of eastern Ukraine this may not pose a problem, but in more populated areas there will be significant targeting friction. If the joint force is digitally integrated, sensors required to validate these targets may be in high demand.

In summary, there are numerous and expanding ways of rapidly detecting hundreds of possible targets by mastering the EMS – even before considering cell network data interception and location, which is not described here. A decision to strike nonetheless carries risk, due to civilian casualty considerations or potentially wasting ammunition on electromagnetic deception. Humans will therefore need to make many of these targeting decisions based on multi-stage processes rather than simply choosing to strike or withholding fire. This is another constraining factor on increasing targeting speed many times over.

Finding Targets with Multi-Spectral Sensing

As noted, signals intelligence may not be sufficient to authorise strikes. For example, direction-finding accuracy **degrades at long range**, and the picture could rapidly become muddied if the enemy deploys false radio or radar emissions. Unless a target is in an unpopulated remote area, targeting cells in brigade, division or corps will require air- or space-based multispectral sensors

and synthetic aperture radar to ensure the strike does not harm civilians or waste munitions.

In current targeting, deciders in targeting cells may require sensors to positively identify targets – both deliberately in the planning phase and dynamically during the operation. This is also a process, because sensors will be subject to competing demands. This is important, because the DTW vision speaks of **automatically matching sensors** to target entities, not only weapons to targets.This could streamline intelligence collection; however, at the same time, deception in the EMS raises the possibility of wasting ISR resources. It does, however, open the possibility of roaming sensors with sufficient edge processing to close kill chains in seconds. For example, a drone can investigate a target detected by a satellite and instantly send coordinates to an artillery unit. In the latter case, there would be **no human involvement** in the kill chain. How then, would such operations unfold in a large-scale conflict with traditional targeting?

Coordinating Targeting Assets

In current NATO doctrine, many of the above considerations – such as whether to jam air defence radars from the air or to stimulate (or unmask) them using ground-launched systems before destroying them – will often involve a process of liaison between staff from component commands, liaison within component commands, and liaison between intelligence staff and targeteers.

In US Air Force doctrine, targeting is described as **'interdisciplinary', 'systemic', and 'estimative'**, and while much of the targeting described above will be highly tactical in nature, there will also be strategic considerations requiring inputs from subject matter experts and, in some cases, international liaison staff. While some discussions may relate to politically sensitive targets (such as captured critical infrastructure or cultural landmarks), decisions by targeting staff must remain aligned with operational plans. Complicating matters, there

is the previously described tension over which headquarters is focused on close or deep operations. Arguably, this tension would be increased by decentralised and accelerated targeting, with weapons typically associated with the close battle increasingly being able to hit enemy force logistics nodes and headquarters, or designating targets for rocket-assisted artillery and platforms comparable to Ukraine's so-called '**middle strike**' systems. In other words, tactical decisions could increasingly carry strategic impact.

Without targeting-staff liaison and coordination of various assets for reconnaissance and strike, decentralised and accelerated targeting risks creating a mechanism for wearing down but not defeating the adversary, with no systemic attack on a centre of gravity. For example, in the drone control station direction-finding problem described above, strike assets held from brigade to corps could be used to find and hit drone ground crews co-located with artillery units. Yet, there is **some evidence** from Ukraine that this can risk diverting ISR to this task at the expense of more impactful activity (such as striking enemy logistics nodes). NATO exercises also provide some **recent evidence** of how ISR can be diverted to less consequential activity.

By contrast, NATO doctrine emphasises corps and divisions attacking targets at depth, which could minimise the tactical drone threat by destroying UAS material on the ground, or by bombing rail yards and bridges so drone units cannot get within range.

Resources will therefore have to be focused. The combination of limited munitions and the ability to find and strike across the force at high speed presents a problem that will probably necessitate planning and component command staff liaison processes described in the first chapter. However, modern targeting technology promises to minimise or even eliminate these processes. Because any digital solution will need to be assessed before action is taken, lower levels will need a high degree of discipline in their targeting

actions, or risk disrupting operations.Liaising targeting staff must also evaluate dual-use targets; for example, cell network base stations may enable enemy usage for UAS and therefore could be struck, but the same cell towers could be critical for friendly forces or friendly civilians.

In most instances, these processes invariably involve some degree of human oversight and interaction, which has led some practitioners to query the extent to which automated targeting decisions could place our own forces at risk as much as challenging adherence to LOAC. This tension is explored in the third section of this paper.

Modern Targeting Frictions

The complexity of modern targeting, both procedurally and technically, contributes to frictions that can impede effective, legal and accurate targeting. All targeting processes involve different degrees and types of friction, but modern targeting – which is unprecedented in its speed and scale of integration – involves a number of new and/or exacerbated frictions.

Many frictions are related to the driving force behind these procedural and technical advancements: the desire for '**decision advantage**'. Decision advantage is the state at which one is making a greater number of better decisions (in this case, targeting decisions) at a faster rate than the enemy. This requires operators to ingest and analyse an ever-greater quantity of data at an ever-faster rate, which now involves a **high degree of automation** through the adoption and integration of **large-scale digitalised systems.** The focus on speed appears to be a common factor in many of these frictions.

Certain frictions prove more consequential than others, as some have potentially affected a military's adherence to legal and ethical constraints. Several scholars have argued that any negative effects of using digitalised

systems to enable targeting are due to the operating procedures of the military in question, and that the use or misuse of these systems will accord with that military's broader commitment to transparency and IHL. These arguments often cite the Israeli Defence Force's **conduct in Gaza**, linking its reported widespread use of **algorithms for targeting support functions** to its historical **tolerance for high levels** of Palestinian civilian harm. Other scholars and legal experts posit that the **use of such advanced digitalised systems** have **inherent risks** that are not being sufficiently addressed. Drawing upon this body of scholarship, this section illustrates many of the tensions, frictions and risks seen throughout modern targeting, especially through the lens of UK targeting modernisation.

Changing Processes and Procedures

Digitalised systems in the targeting process act, first and foremost, as integration and workflow aids. What was previously a series of disparate systems using vast staffs to collect, transfer, update and analyse data across domains has now been cohered into one or more common software platforms, such as the **Maven Smart System** in the US and NATO, or **Avengers** in Ukraine. These platforms promise higher efficiency and efficacy, **facilitating interaction between systems and domains** at a speed and scale impossible for unaided human operators. Such systems reduce the number of targeting staff needed, as many tasks become automated or redundant.

Within the UK defence sector specifically, there is a lack of consensus about the degree to which initiatives like the DTW will change modern targeting platforms and workflows, as well as how significant such changes would be to targeting processes. Many policymakers and some practitioners have described the DTW as essentially implementing **Network Enabled Capability** concepts, with one senior policymaker saying that modern targeting policy is 'nothing fundamentally different' to that of recent decades.[2] Indeed, while the UK

Ministry of Defence (MoD) is releasing new policies related to the responsible use of modern digital systems (namely **JSP 936**), targeting policy remains grounded in traditional policy documents (such as the **JSP 398**, **JSP 900** and **NATO AJP-3.9**).

There may be some areas where, even if the policy is sufficient, the practice around its implementation will require changes. For example, the delegation of authority remains strongly influenced by expectations from the Global War on Terror. Commanders, civil servants and even ministers have grown accustomed to being intimately tied into sensitive operations. This has been (mostly) manageable where the tempo has been lower and where the targeting has involved planning over weeks or months. However, in the event of a high-intensity war with hundreds of strikes each day, such a level of involvement will not be possible, especially if operating in a contested and congested communications environment. But, in the words of one MoD official, 'BDA [Battle Damage Assessment] is instantaneous on social media, leading to demands of accountability from ministers'; this is likely to further reduce the risk considered tolerable in ministerial guidance, even as the battlefield might demand more delegation.

In the event of large-scale operations, the decision-making authority for most strikes, especially for targets of opportunity, will have to be devolved to mid-level or even junior commanders in the field. Commanders will inevitably take action that – whether intentional or not – causes significant civilian harm and/or escalation in enemy response. MoD officials and ministers must grow accustomed to these realities of modern operations, where they will bear the political consequences for actions outside their control. Commanders, in turn, will have to become more comfortable delegating authority to more junior commanders, further stretching the bounds of mission command. In both cases, the risks of insufficient deconfliction and delegation at the appropriate levels could range from incoordination, leading to failure of mission objectives,

to unintended civilian harm or fratricide. Current targeting processes, with guidance over who performs the role of what, is known as **target engagement authority**, which takes account of these challenges and provide guidance as to who performs which role. The issue is therefore less about process and more about habit and culture: senior officials and ministers will have to become more comfortable with delegation and risk, or at least be more precise in the parameters they set out for targeting.

Conversations with practitioners and industry experts present a more complicated picture of policy. As digitalised systems come to further integrate and perform functions of targeting, they may become inextricable from the very policies guiding the process. As the DTW is still in its early stages, how these workflows and functions will be structured remains unclear, to say nothing of the technical architectures underpinning and integrating the MoD's different areas. Absent a centrally-driven view of what the targeting process will look like when it is mature, certainty about the sufficiency of existing policy appears premature. Indeed, practitioners often lack a uniform understanding about how their role in this process will change as the DTW is implemented, including around areas like automation, considering MoD's Defence Targeting Enterprise (DTE) description of one of its strategic principles as 'automation by default, human by exception'.[3.]

Human-Machine Teaming

Despite these challenges, NATO militaries are committed to increased automation within the targeting cycle, albeit with **diverse and often controversial approaches** to the human role in the process. National policies vary regarding the acceptance of **'full' autonomy**, with the UK focusing on '**context-appropriate human involvement**' as a manner of implementing '**meaningful human control**'.

A full elucidation of the dynamics of autonomy in targeting is outside the remit of this paper, but Table 1 provides a typology of the many potential frictions involved in human–machine teaming in targeting functions. These frictions are temporally dynamic, meaning friction mitigation efforts cannot be static.

Table 1: Areas of Potential Friction in Human–Machine Teaming

LEGAL & ETHICAL	Legal and ethical acceptance of degrees of autonomy
	Diffusion of authority, attribution, and responsibility across commanders, designers/technicians and operators
	Visibility and auditability of decision-making
	Institutional mechanisms of accountability for errors, mistakes or misuse of systems
HUMAN	Understanding of technical systems
	Understanding of systems' weaknesses and limitations
	Trust in system fidelity
	Trust in one's operation of the systems
	Confidence and cognitive biases
	Time and cognitive space to assess outputs
STRUCTURAL	Authority and ability to challenge system outputs
	Narrowing and constraining of human judgements by machine [interface]
	Team coordination on roles and systems' sharing
	Strike authorisation clarity
	Escalation risks, whether accidental, inadvertent or deliberate
	Contingency and redundancy processes in the event of system failure
ALIGNMENT	System alignment with operator/commander's intent
	Ontological alignment between human and systems
	System alignment with reality
	Automation effects on human alignment/connection to reality

Credit / The authors.

Safeguards

The most public controversies about the integration of digitalised systems, especially AI, into targeting processes centre around whether such systems strengthen or degrade protections built into the processes. Algorithmic-assisted/guided targeting functions promise a vision of targeting that is both more accurate and more discriminate due to the exponential increases in the amount of data processed per target. In theory, the replacement of error-prone humans by high-fidelity algorithms could enable greater certainty of positive identification, better weaponeering for sensitive targets and a greater likelihood of accurately calculating potential civilian harm. However, this vision remains elusive, in part because it requires robust safeguards to remain in place and even improve, given the **new set of vulnerabilities** in modern digitalised systems.

Putting aside technical considerations around the **accuracy, testing and assurance** of these systems, which are outside the remit of this piece, the core concerns stem from debate about the necessity of ever-increasing speed in targeting. Many legal and humanitarian experts oppose the **primacy of speed** in targeting, on the grounds that it will undermine legal and ethical checks as well as technical assurance of systems. The logic is simple: a compressed timeframe to make a decision, whether largely by a machine or a human, reduces the ability to perform robust reviews.

Many practitioners and policymakers do not share this concern. Instead, a number of practitioners expressed their doubts about the need for such rigorous legal and ethical safeguards in such processes. A frequent claim expressed in conversations and interviews is that since the UK's/NATO's enemies do not feel bound by such rules, the slowing of one's own operations by these safeguards presents an unacceptable risk on the battlefield.

This tension is evident across the MoD, with civil servants and operators attempting to balance between speed and safeguards. Policy leads in the MoD described their work to 'increase the speed and capacity [of targeting] while maintaining quality'.[4] Comments like this are not uncommon, where increased speed and scale are juxtaposed with legal and ethical priorities in an attempt to maximise both.

However, the UK DTW's core team took the concept further, listing one of the DTW Strategic Principles as: 'assurance, legalities, ethics and security must accelerate tempo, not constrain it.'[5] On its face, the statement fundamentally misunderstands the purpose of safeguards, which by their nature slow down processes. Technical assurance processes, legal reviews and security protocols are extra steps added into targeting procedures, thereby increasing the steps and time needed for a cycle to complete. Even if partially or wholly automated, safeguards cannot be expected to increase the speed of a targeting cycle any more than friction can be expected to increase the speed of a moving object.

To be fair, there is a dearth of detailed public data about the sufficiency or insufficiency of checks in recent operational digitalised targeting. As put by one scholar, **one could empirically test** whether modern targeting in ongoing conflicts using cutting-edge digitalised systems has been performing all critical checks sufficiently. Ideally, armed forces are carrying out their own internal post-operational assessments to perform these empirical tests and adapt accordingly, although this requires robust internal accountability mechanisms and a willingness to **engage with the public** about errors and mistakes.

Technical civilian protection tools can be **embedded into such targeting workflows**, but it remains unclear when or if such tools are used. Furthermore, the efficacy of such tools will probably vary drastically depending on the system's manner of technical and workflow integration, training and operational data available, and organisational prioritisation of IHL in operations.

Despite the gaps in information, ongoing conflicts have still provided a high level of data about targeting, where lessons can be drawn about the sufficiency of these safeguards for civilian protection. At the time of this research, US and Israeli strikes on Iran have hit thousands of sites, causing **widespread destruction to both military and civilian objects, and killing over 2,000 civilians.** In some of these cases, the damage was intentional, demonstrating a high degree of tolerance for collateral damage even while some of the strikes might be considered causing **disproportionate harm under IHL.** In other cases, such as the **strikes on the Minab school** that **reportedly** killed over 150 civilians (mainly children), **human error has been blamed.**

Advanced digitalised systems appear to enable the speed and scale of such actions, both intentional and accidental. It remains difficult to separate the civilian toll from the public decision by the US Department of War to **cut civilian protection offices** in the Pentagon in favour of prioritising '**maximum lethality, not tepid legality**'. Such incidents should concern the MoD, which has recently **highlighted the vulnerabilities** of its own Civilian Harm Mitigation and Response policies and processes.

Technical and Tactical Faith

Beyond the operational frictions described above, the primacy of targeting speed and scale can lead to officials having misplaced faith in the value of these actions. The US and Israeli war with Iran and **Israel's war on Gaza** have been historic in the speed and scale of their targeting, killing many thousands of combatants and crippling military (and civilian) infrastructure. Yet, in neither case can the result be (yet) considered a strategic victory.

Modern targeting capabilities sit at the centre of modern militaries, doctrinally, procedurally, financially and operationally, exerting a gravity across the whole of the force. Commanders, analysts, operators and even policymakers are drawn to the near-perfect situational awareness and near-instantaneous kill

chains as the solution to information and decision advantage. However, decision-making still needs situating in clear strategy and achievable campaign goals, rather than being driven by the logic of one's advanced technical means.

Regardless of advances in automation and digitalisation, warfare will remain a human affair, contextualised by human perceptions, and more often won in political choices than physical ones. Effective military decision-making requires political, sociological, cultural and legal considerations, all of which become **brittle when quantified.** Prioritising quantifiable metrics – such as a goal of 'XX targets in XX time'[6] – can enable greater lethality, but risks excising the human perceptions, judgements, reactions and ingenuity without which a war cannot be won.

Prioritising quantifiable metrics – such as a goal of 'XX targets in XX time' – can enable greater lethality, but risks excising the human perceptions, judgements, reactions and ingenuity without which a war cannot be won.

Conclusion

A high-intensity confrontation in the European theatre would present British and European Allied forces with difficult targeting decisions on a scale that arguably has no recent parallel in their experience. Emerging technology creates opportunities for ongoing modernisation efforts even as grinding frictions could stymie targeting scale and speed ambitions.

Broadly, engagements with industry and practitioners in the context of this paper described potential tensions stretching from the highest strategic levels,

where the desire to neutralise enemy threats at depth could clash with a political desire to oversee individual strikes and operations. Such a problem is not new to large-scale, integrated operations. Indeed, during the Kosovo crisis, there were **protracted debates** on the extent that coalition forces should strike Serbian infrastructure or focus attacks on Serbian forces.

To an extent, the UK's DTW initiative promises to reduce such frictions, analysing surges of targeting data to find vulnerabilities in the enemy force, shifting a burden of human analysis to machine work. Yet, as the campaigns described in this paper – from Gaza to Iran, and Kosovo before – illustrate, responsibility for decisions will always rest with the humans involved.

It is possible, therefore, to imagine a campaign where targeting decisions may require political sensitivity which stands directly at odds with a highly decentralised and compressed 'sense, decide, effect' cycle. This is not to say efforts such as the DTW initiative will be rendered ineffectual in such circumstances, but expectations of massive increases in target generation must be managed.

Furthermore, decisions must be made now as to how the DTW will operate in a coalition with similar capabilities. Current British and French thinking appear to be gravitating towards a re-focus on **destroying the enemy at depth.** Almost by definition, this will involve targeting areas close to dual-use infrastructure. Unless there is a high degree of interoperability among Allied targeting capabilities, and a shared understanding of how to fight a campaign, the political implications of some targeting decisions described in the first section of this paper may increase targeting friction.

Imagining the full DTW capability therefore implies aligning targeting policy and procedure between Allies, now rather than later. The DTW capability aim of interoperability with Allied equivalents is vital, especially if brigades or even battle groups are able to fight what was traditionally the deep battle. Indeed, if

we expand this risk of insufficient interoperability, there remains the possibility that certain targets could be prosecuted multiple times by Allies using limited, exquisite weapons. Targets which one force may identify as posing a collateral damage risk may be erroneously identified by an unconnected Allied targeting system as legitimate sites to strike. Other problems, such as deconfliction, would be complicated in the absence of highly interoperable targeting capabilities among Allies.

Last, there remains uncertainty as to how we will fight in a synchronised way in accordance with careful planning processes if the capability reaches the full potential of complete force connectivity, especially as dispersed units, potentially operating in radio silence, can strike at increasingly vast distances.

Many of the problems described here in joint force integration are not new, but, in the UK, the DTW's ambitious goals mean they could soon affect how we fight. This raises profound implications for training and doctrine which must be addressed before the onset of conflict.

Acknowledgements

This project is possible through generous support from Fujitsu, Leonardo, Systematic and Thales. RUSI retains its independence in research outputs, which represent the authors' views alone and do not represent any institution.

WRITTEN BY

Robert Tollast
Research Fellow, Land Warfare
Military Sciences

Noah Sylvia
Research Fellow, C4ISR and Emerging Tech
Military Sciences

Matthew Savill
Director of Military Sciences
Military Sciences

MEDIA ENQUIRIES

Jim McLean
Media Relations Manager
+44 (0)7917 373 069
JimMc@rusi.org

Footnotes

1.:
Author conversation with intelligence expert, in person, April 2025.

2.:
Author conversations and interviews with experts, officials, service members and industry leads, in-person and online, 2026.

3.:
'Digital Targeting Web Industry Day' slides, Defence Targeting Enterprise, March 2026.

4.:
Conversations with MoD officials, in person, February 2026.

5.:
'Digital Targeting Web Industry Day' slides, Defence Targeting Enterprise, March 2026.

6.:

‘Digital Targeting Web Industry Day’ slides, March 2026.