The Digital Targeting Web
Challenge Book 2026

National Armaments
Director Group

Cyber & Specialist
Operations Command

Contents

Introduction

Targeting is the core of military activity: the command process that links understanding, decision making and the orchestration of activity to delivery effects.

This process is fuelled by data and it is only by creating the digital environment to allow data to move freely that the Armed Forces will be able to fight fast enough to over- match adversaries, as a coherent, integrated force.

The Digital Targeting Web is at the core of the Integrated Force, it will transform how Defence operates.

Why do we need the Digital Targeting Web?

The UK needs a Digital Targeting Web (DTW) to enable success in modern conflicts. To outpace adversaries, we must sense, understand, decide, act, and assess faster than they can.

This process relies on data, which must be collected, shared, and used efficiently to support targeting and Command and Control. Current systems need to evolve to allow seamless data flow and automation, creating a competitive edge.

The Digital Targeting Web must be flexible, robust, work with any technology provider, and function reliably in environments with electronic warfare challenges.

The opportunity for Defence

The DTW improves the speed and efficiency of targeting, Command and Control (C2), intelligence, surveillance, and situational awareness on the Digital Backbone, supporting successful operations.

By focusing on data across the entire C4ISTAR system and enabling large-scale information sharing across all levels, classifications, and domains, it allows us to act faster than our adversaries.

The DTW will set targeting standards, combine data from multiple sources and tactical links into near real-time common operating pictures, and support advanced analytics, automation, and machine learning.

It will also enable AI to deliver deeper strategic insights and shared tactical awareness, while enhancing international collaboration.

The Digital Targeting Web | Challenge Book 2026

The Digital Targeting Web Vision

An adaptive, secure and evolving set of digital services that unite users, systems, and platforms to enable targeting accuracy, precision, speed, and resilience across all domains.

The DTW Challenge Book

This document has been developed in partnership with stakeholders from across the MOD. It has taken the issues and problems that users face when trying to digitise their targeting work and translated them to clear challenges. The challenge book will be key in communicating with industry. It is intended to focus engagement with industry partners in the search for new ideas and technologies that support the achievement of the Digital Targeting Web vision. The DTW challenge book is an evolving document that will be periodically reviewed to best reflect the evolving targeting landscape. The details contained within the document, whilst representative, are non-exhaustive and are limited due to classification.

Challenge Book Guiding Principles

The challenges are guided by several overarching criteria:

1. **Workflow-Driven Transformation:** Focus on workflows that deliver measurable speed, scale, and precision. Prioritise operational value over infrastructure-first efforts, using standards, incentives, and telemetry to govern change.

2. **Leverage Existing Assets:** Build on Defence's existing technical estate and Digital Backbone to maximise value from prior investments while adapting and enhancing capabilities.

3. **Assume automation; prove trust:** Design for machine-speed operations with automated processes, policy-as-code, explainability, immutable audit trails, and resilience mechanisms. Trust must be proven through robust security and transparency.

4. **Data-centric by default:** Treat data as a strategic asset: discoverable, accessible, understandable and trusted (DAUT). Enforce metadata, lineage, quality SLAs, and cross-domain sharing.

5. **Open, Interoperable, and Modular:** Use open architecture and modular designs to ensure compatibility across platforms, allies, and systems, supporting NATO interoperability and rapid integration of new technologies.

6. **Semantic Sovereignty:** Retain ownership and control over data ontologies to ensure consistent interpretation and protect intellectual property critical to Defence operations.

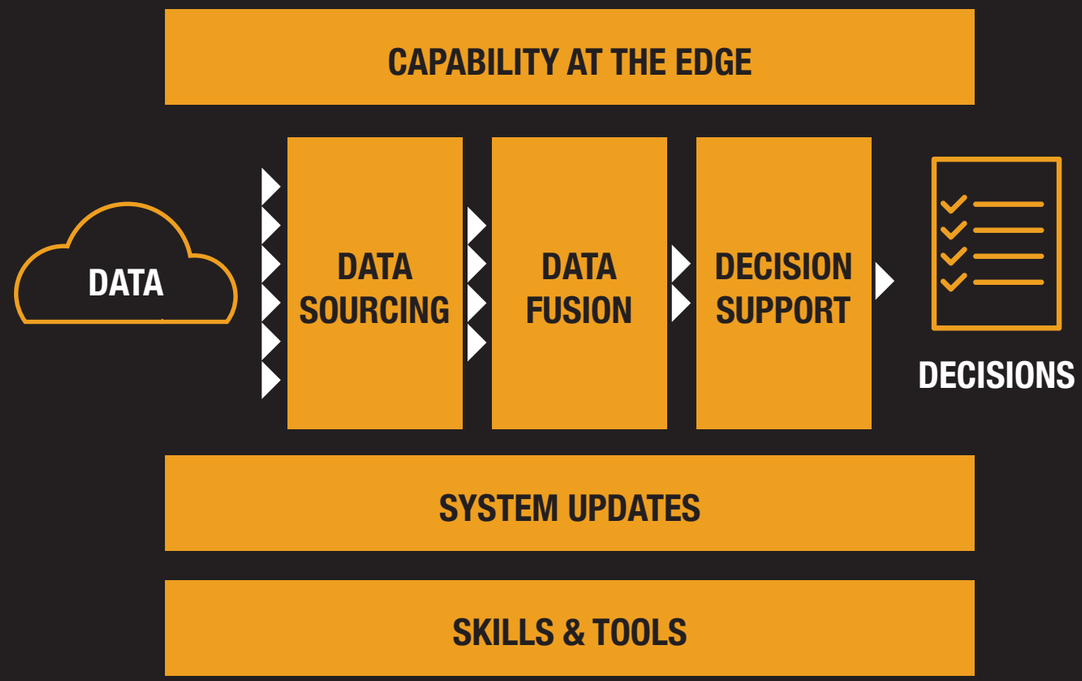
7. **Decentralised operating model; federated governance.** Operate as an ecosystem with lightweight central orchestration, domain-owned products and shared trust frameworks.

8. **Collaborative and Adaptive Development:** Foster partnerships with industry, academia, and allies to deliver user-focused, innovative, and continuously improving solutions that adapt to evolving threats and operational needs.

9. **Security and Resilience by Design:** Embed security and resilience into all designs, including zero-trust principles, adversarial testing, supply chain assurance, and hybrid cloud/edge solutions for disconnected operations.

Digital Targeting Web Challenges

Getting from data to decisions faster



Securely sourcing and sharing data between dispersed and siloed locations

Challenge 1

Challenge 1

Securely sourcing and sharing data between dispersed and siloed locations

Description. The UK military faces significant challenges in efficiently sourcing and sharing critical data that is dispersed across multiple siloed systems, applications and locations. This fragmentation undermines operational effectiveness, collaboration, and timely decision-making, which can negatively impact mission success and resource allocation. Addressing this challenge requires enabling the seamless sharing of data from a variety of sources, across classifications, digital and geographic locations, and alliances through a move to data-centric interoperability.

To do this introduces difficulties. Maintaining the different rules for sharing and accessing different data. Preserving the security protections required for different sources. Securely bridging the gaps between different siloed networks. Managing the connection to Denied, Disrupted, Intermittent and Limited (DDIL) data sources. Assuring that the data received is correct and has not been corrupted in transit.

Questions to answer.

- How can resilient access to data sets be maintained in a DDIL (Denied, Degraded, Intermittent, or Limited) environment?
- What strategies can be used to prioritise data sharing between buckets when bandwidth is restricted?
- How can data be securely and effectively shared across domains with differing classifications, nationalities, locations, and ownerships?
- How can identity verification be reliably established and maintained in a contested environment?
- How can data governance be automated, delivered at pace, and designed to enable rather than restrict access?

Our key focus areas are:

Data Sourcing 1. Defence needs a way to connect the Sensor-Decider-Effector kill chain which can be replicated across Tactical, Operational and Strategic Headquarters (HQs) to enable targeting at scale and speed.

Operational Parameters

- Must be able to quickly share multi-source, multi-classification data via common data-centric applications.
- Useable within a NATO construct and able to incorporate sovereign and multi-lateral data feeds.
- Must operate within relevant Emissions Control (EMCON)/Counter Surveillance Control Measures (CSCM) states.
- Should include backup of essential mission data, providing resilience within the system.

Operational Use Case

As part of a deployed NATO task force in the High North. UK commanders face an enemy with significantly improved offensive targeting capability resulting from recent warfighting experience. To prevent overmatch, 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. UK forces must be capable of connecting with allies securely, drawing data together to maintain an advantage even when an enemy skilled in denial and disruption of communications degrades our capability to operate. This data must be drawn together into trusted products capable of rapid sharing, reducing decision making time whilst overcoming the complexities inherent within legacy and allied data systems.

Challenge 1

Securely sourcing and sharing data between dispersed and siloed locations

Data Sourcing 2. The MOD needs a way to connect its data systems with those of NATO, intelligence services, and non-traditional partners to enable seamless collaboration and decision-making across different systems, security levels, and operational domains.

Operational Parameters

- Must be able to quickly share multi-source, multi-classification data via common data-centric applications.
- Must be fully compatible with NATO standards and capable of integrating sovereign and multinational data feeds.
- Must function reliably and resiliently, even in contested or degraded environments.

Operational Use Case

Long-standing political tensions Europe escalate into a fast-moving crisis: NATO mobilises. The response includes the military, national intelligence agencies and other partners who each hold key information: satellite imagery, classified intelligence and real-time updates. As the situation deteriorates commanders from the UK contingent utilise an interoperable network to securely access and fuse these disparate data sources across national and organisational boundaries without compromising handling protocols. This is achieved in a hostile environment contested by highly capable, sub-threshold adversary. With a secure, shared, and coherent operational picture established, NATO commanders can coordinate planning, adapt to emerging threat, and conduct effective operations in real time.

The Digital Targeting Web | Challenge Book 2026

Data Sourcing 3. The UK requires a capability to coordinate targeting efforts seamlessly across allied and partner nations, ensuring interoperability and shared situational awareness to enable effective joint operations.

Operational Parameters

- Must enable the rapid flow of targeting data between the UK and allied nations to support dynamic targeting.
- Using NATO standards to pass UK targeting data direct to allied effector based on prioritisation.
- Must maintain data-centric interoperability between NATO nations preserving the security and integrity of the source data.

Operational Use Case

In response to an uptick in political tensions between NATO and our adversary, Headquarters Allied Rapid Reaction Corps (HQ ARRC) deploys in Europe. The UK takes the lead in coordinating NATO joint effects in a specific area, drawing targeting information from multiple nations. As our adversary concentrates forces within reach of border areas, UK commanders must effectively fuse a range of nationally derived and NATO data to direct and coordinate complex NATO formations and personnel across the battlespace in anticipation of escalating hostilities, whilst effectively mitigating the risk of miscalculation.

Combining data sources
to produce information
and generate insight

Challenge 2

Challenge 2

Combining data sources to produce information and generate insight

Description. Once disparate data sources are connected, there is a need to combine and process them to create actionable information and valuable insights. These information feeds, including open-source data, should be tailored to the user's role and credentials, ensuring they receive the insights necessary to address their specific problems. This challenge highlights the importance of streamlining access to the right information at pace.

To do this introduces difficulties. The data that the user has access to could depend on both their personal and role profiles. Access to some data may be time sensitive. Users may have limited access to the data due to their physical location. Co-location of data sets is highly unlikely to be possible due to ownership and classification.

Questions to answer.

- How do we combine and fuse data to generate information/insight?
- How do we turn data into information and then intelligence?
- How do we maintain handling caveats when data is turned into information & intelligence?
- How do we assure the provenance and integrity is maintained when sources are combined?
- How do we automate and accelerate the generation of information & intelligence?

The Digital Targeting Web | Challenge Book 2026

Our key focus areas are:

Data Fusion 1. Automate and expand data sources, automating the identification and collection of data from multiple sources (open-source intelligence, surveillance systems, partner networks, sensors, etc.) into one data feed that addresses the current threat. Processing these feeds into a curated set of information to improve targeting, analysis, and decision-making, making operations faster and more flexible.

Operational Parameters

- Needs to be compatible with existing infrastructure.
- Needs to ensure data integrity and traceability of source information.
- Should be interoperable across a wide range of data source.

Operational Use Case

When deployed on operations, UK forces automate the identification and collection of data from diverse sources – including open-source intelligence, surveillance systems, partner networks and sensors. The tooling automatically integrates these inputs into a unified data feed, capturing evolving battlespace threats in real-time, transforming it into actionable intelligence. Battlespace decision makers access this data in a consumable way and authorise courses of action with confidence due to accurate targeting and improved situational awareness capability.

Challenge 2

Combining data sources to produce information and generate insight

Data Fusion 2. Coalition partners able to operate in the same digital environment as MOD on collaborative operations. They are given access to the data that is needed for the mission, and they are entitled to see. This should enable the partner nations to contribute to and collaborate on targeting. Access should be brokered not only for people but for systems and software as well.

Operational Parameters

- Access should be dynamic based entity characteristics.
- Access should be both time and context dependant.
- Solutions should be able to consider people and systems.
- Should automate large parts of the access control.

Operational Use Case

Whilst under NATO command the UK Carrier Strike Group takes the lead in co-ordinating targeting efforts. Data is shared autonomously and dynamically between allies based on operational need and handling protocols in response to increasingly aggressive adversary naval posture. This ensures that data is drawn from the full spectrum of NATO nations whilst targeting information is effectively distributed to an appropriate effector.

Data Fusion 3. The MOD needs a way to enable assisted target development through the Find, Fix, Track, Target, Engage, Assess (F2T2EA) process, supporting multi-domain targeting to identify and neutralise high-value targets in dynamic and contested environments

Operational Parameters

- Must automatically identify targets using all-source data.
- Must enable rapid target identification within contested and denied environments.
- Requires a master entity catalogue and semantic ontology mapped to data sources.
- Must present potential targets to users automatically.
- Must support the planning of Courses of Action (COAs) and focus operational efforts.

Operational Use Case

Royal Navy vessels deployed alongside allies continuously monitor a congested and contested battlespace using a wide range of sensors including satellites, drones, and electronic warfare systems. As the data arrives, the system automatically pulls these feeds together, filtering out the noise. Information moves smoothly across domains and security levels, so staff can work from a shared, real-time picture even when in degraded or denied environments. Refined targeting data and the ability to match targets to effectors aids Commanders in shaping viable courses of action.

Building knowledge from information and making decisions faster

Challenge 3

Challenge 3

Building knowledge from information and making decisions faster

Description. To develop the information generated by the Digital Targeting Web (DTW) in knowledge, users and decision-makers must be equipped with the right tools to analyse and present effectively. This ensures that the best course of action is clearly communicated. Addressing this challenge supports the need to provide decision-makers with timely insights to make critical decisions within shorter timeframes.

To do this introduces difficulties. The access to the infrastructure normally available through cloud computing may be severely restricted at the edge. Access restrictions and caveats need to be maintained and enforced in the information generated. Access to common internet based and SaaS tools is unlikely to be available at higher classifications.

Questions to answer.

- How do you provide decision support to increase the pace of decision making whilst maintaining the integrity?
- How do you present knowledge and insights in a way that is consistent, accessible, and actionable?
- How do you quickly generate and maintain robust and trustworthy records of decisions?
- How do present an assured and auditable record of the digital decision chain?
- How do we leverage knowledge outputs from the process to achieve the desired effect?

The Digital Targeting Web | Challenge Book 2026

Decision Support 1. Users of the DTW need a method to support the visualisation of Targeting Products. There needs to be a move from long static document-based approaches to ones that accelerate decisions making. Targeting products to more dynamic visualisations that more clearly present meaningful and valuable intelligence to decision maker.

Operational Parameters

- Should be quicker and easier to use than current manual processes.
- Should be intuitive to both those developing the products and those that are consuming them.
- Should maximise re-use of existing and emerging infrastructure.
- Needs to ensure data integrity and traceability of source information.

Operational Use Case

Complex datasets are transformed into clear, actionable insights that can quickly and easily be communicated to decision makers. Using geospatial mapping, heatmaps, and timelines, analysts can visually represent key intelligence, such as enemy positions, movement patterns, and terrain analysis. Multi-source intelligence is the norm, fusing several feeds of disparate data into a cohesive operational picture. Improved situational awareness supports precision targeting and ensures informed decision making, ultimately enhancing mission effectiveness and reducing operational risks

Challenge 3

Building knowledge from information and making decisions faster

Decision Support 2. Using Human-Machine Teaming in targeting cycle to reduce the end-to-end time taken to perform a targeting lifecycle process workflow in a defined mission thread or vignette. Integrating human decision-makers with AI and autonomous systems to enhance targeting accuracy and speed. Using artificial intelligence and machine learning to process vast amounts of data, identify patterns, and accelerate decision-making in targeting workflows.

Operational Parameters

- Robustness and integrity of decisions need to be preserved.
- Users need to trust the outputs through transparency and reliability.
- Compute is likely to be limited at the edge.
- Humans need to remain in the loop, augmenting decision making rather than taking the decisions.
- AI support operates within the legal framework established for targeting.

Operational Use Case

In future high-tempo conflict, UK forces deploy AI-enabled systems to streamline the targeting process. ISR platforms collect vast amounts of data, which AI rapidly analyses to identify potential threats. Machine learning algorithms prioritise targets based on risk and mission objectives, providing commanders with real-time recommendations. Human operators validate AI outputs, ensuring compliance with rules of engagement. AI dynamically re-tasks drones for continuous surveillance, while predictive analysis anticipates enemy movements. Edge computing enables rapid decision-making in the field, reducing reliance on centralised systems. This human-machine collaboration shortens the targeting cycle, enhances precision, and allows forces to respond faster to emerging threats.

The Digital Targeting Web | Challenge Book 2026

Decision Support 3. Making use of advanced analytical tools to undertake complex systems analysis and vulnerability targeting. Automatically identifying and assessing vulnerabilities in complex systems and determine attack vector planning options. Looking at kinetic and non-kinetic targeting options in typical operational, hybrid warfare and grey zone scenarios.

Operational Parameters

- Electronic warfare and information operations to disrupt, degrade, or influence adversary capabilities and decision-making.
- Addressing unconventional threats, such as disinformation campaigns and economic coercion, through tailored targeting approaches.
- Identifying and neutralising adversary networks, systems, and infrastructure through offensive cyber operations.

Operational Use Case

In response to a resurgent terrorist presence in the Levant, MoD decision makers access advanced tools that analyse complex systems revealing hidden vulnerabilities, and present viable kinetic and non-kinetic targeting options. The tooling compares effects and helps users choose the most impactful course of action in the most efficient manner. This will include effectors aimed at degrading or influencing adversary capabilities and networks, often enabled and coordinated through partners and allies to maximise effect.

Providing the Digital Targeting Web at the Edge

Challenge 4

Challenge 4

Providing the Digital Targeting Web at the Edge

Description. The DTW must enhance decision-making speed across the enterprise, extending beyond the core to users at the edge. It should provide access to the same data, tools, and services (or critical elements thereof) while ensuring that essential data or information is returned to the core. In austere environments, the system should gracefully degrade, prioritising critical elements to maintain operational effectiveness. As connections are restored systems and services are re-synchronised and critical data prioritised.

To do this introduces difficulties. There will be limitations in both networking and compute at the edge. The systems and services in the DTW need to continue to function during period of Denied, Disrupted, Intermittent and Limited (DDIL) communications and synchronise data as they are reconnected. Access to SaaS & Cloud hosted services is likely to be limited at the edge.

Questions to answer.

- How is access to DTW tools and services maintained at the edge?
- How is a common time reference maintained across the DTW?
- How is bandwidth use prioritised to maintain critical functionality?
- How is data stored, processed and cached at the edge?
- How does the DTW synchronise when connections are restored?
- How can cloud based services be accessed or replicated at the edge?
- How is confirmed identity achievable and stable in a contested environment?
- How does the DTW maintain resilience whilst networks are being degraded and destroyed?

Edge 1. Providing mission-aware prioritisation and queueing of data and tasks. There is a need to dynamically prioritise, queue, and route ISR data based on mission context to ensure that the most critical information reaches decision-makers and effectors first, even when bandwidth is limited or contested. Implementing store-and-forward mechanisms that allow ISR data to be temporarily held and then forwarded when connectivity improves, ensuring continuity of targeting operations without data loss or operational paralysis.

Operational Parameters

- Should operate effectively under intermittent or degraded connectivity (e.g., EMCON/CSCM).
- Needs to be compatible with existing infrastructure.
- Should support multi-path delivery and intelligent retry strategies.
- Needs to ensure data integrity and traceability throughout the process.

Operational Use Case

During a high-tempo operation, a surge of ISR data arrives from multiple sensors. The system automatically prioritises targeting data related to imminent threats, ensuring it is delivered to commanders and effectors ahead of less urgent information, even as network conditions fluctuate. A forward-deployed unit loses connectivity during a mission. The system stores incoming ISR data locally and, once a connection is re-established, automatically forwards the backlog to headquarters and relevant effectors, maintaining the operational picture and supporting rapid targeting decisions.

Challenge 4

Providing the Digital Targeting Web at the Edge

Edge 2. Ensuring that deployed users have adequate access to the infrastructure provided to undertake complex tasks such as AI at the Frontline. Provide a way to access advanced compute and storage directly in the field to process data at an appropriate speed. Supporting the need for frontline units to make fast decisions without needing to send data back to headquarters or the UK for processing.

Operational Parameters

- Fast-moving or disrupted environments.
- Restrictions on Size, Weight & Power (SWaP) due to operating conditions.
- Limitations in the service are expected however it should gracefully fail.

Operational Use Case

Whilst operating in the High North Royal Navy assets and task groups can rely on the DTW. Even in these remote and hostile environments, task groups and ships will rely on the DTW to adapt dynamically, ensuring mission-critical data reaches commanders and effectors without delay. This is despite of these operations facing communications challenges due to limited geostationary satellite coverage, ionospheric disturbances, and vast distances.

Edge 3. The Forward Land Forces need a way to use existing equipment like unmanned systems, vehicles, or sensors to gather and share real-time information to build a Common Operating Picture which enables better decision making.

Operational Parameters

- Must utilise passive data transmission with minimal user interaction.
- Needs to be compatible with existing infrastructure.

Operational Use Case

After a series of border incursions into a NATO country, a deployed UK combined arms Brigade conducts a complex obstacle crossing deep within contested territory. In order to understand where flanking friendly troops are located and make an appropriate and timely decision regarding battlespace movement, the Brigade pulls information from equipment, such as UAVs and existing sensors, to form a real-time picture of adjacent friendly activity at pace and with high confidence.

Upgrade, integrate and interoperate at pace

Challenge 5

INTEGRATED WARFARE CENTRE

Challenge 5

Upgrade, integrate and interoperate at pace

Description. The DTW must be capable of adapting to changes in threats, operational areas, and the availability of new data and tools. It should rapidly integrate new tools and models as they become relevant while maintaining interoperability with an evolving set of data sources. This challenge underscores the need for continuous improvement to ensure the DTW remains fit for purpose and meets user requirements.

To do this introduces difficulties. The infrastructure available at higher classifications is likely to be limited and will not be able to access services outside of that domain. The capability should be designed in way where it can quickly adopt both emerging tools and those that don't exist yet. There must be a way to ensure the integrity of the system is maintained during changes to preserve safety and legality.

Questions to answer.

- How do we test and assure data models for use within our systems?
- How can standards be used to help rather than hinder or restrict?
- How do we manage change and interoperability with partners?
- How do we manage assurance and accreditation dynamically?
- How are reliability and availability provided in a dynamic system?
- How do we interoperate with a wide range of sensors and effectors that we may or may not own?
- How can we deliver tools into operational environments?

The Digital Targeting Web | Challenge Book 2026

System Update 1. Users need metadata to be harmonised across different data sources and intelligence products. The DTW needs to ensure that ISR data from different sources is described using harmonised metadata, so it can be easily discovered, fused, and exploited across the system.

Operational Parameters

- Must not prescribe a single metadata schema but should enable mapping and translation between schemas.
- Should support both legacy and new data sources.
- Needs to be compatible with NATO and allied data standards where feasible.

Operational Use Case

An analyst is tasked with tracking the movement of a terror group's refined oil in the Levant destined for the black-market as terrorist funding. The analyst can easily fuse satellite imagery with ground-based sensor tracks. Using harmonised metadata, the analyst's tools automatically align and correlate data from multiple sources to create a consistent picture of the terror group fuel convoy. They are confident that the target is consistently identified regardless of the data source. The targeting process is accelerated through the large reduction in the amount of manual data wrangling required.

Challenge 5

Upgrade, integrate and interoperate at pace

System Update 2. How is confidence and integrity maintained in an evolving system. Dynamic system assurance will be needed to preserve the systems safety and legality. The explainability of the systems will be required to underpin trust in it.

Operational Parameters

- Automated and explainable impact assessments.
- Evidence captured for future review or scrutiny.

Operational Use Case

Duty holders have confidence in the safety and legality of the DTW as changes are made and services added. Despite it being an evolving digital system when updates or modifications are made any new risks are understood and the integrity of the outputs are preserved. It is easy to quickly understand the impacts of changes without having to rely on long and process driven assurance. Continuous autonomous reviews of updates or modifications enable the duty holder to assess operational risk associated with DTW and make informed decisions on the use of its outputs.

System Update 3. Users are able to combine the DTW with modelling and simulation inputs to enable the development and refinement of standard operating procedures and the virtual testing of introducing new capabilities. As new detectors and effectors are introduced, their potential applications can be rehearsed, tested, and refined within the DTW before they are fielded. Allowing for the for mission rehearsal with capabilities that are still in development enhancing preparedness and linking directly to increased confidence in operational outcomes.

Operational Parameters

- Correct classification of system to be employed.
- Weapon system real world parameters to be protected.
- Not to impact the operation of the operational DTW.

Operational Use Case

Testing of new weapon systems is enhanced by feeding modelling and simulation data into the DTW. Supporting in the validation of the capability and its operational use before it is deployed. Allowing additional virtual testing to be conducted to a greater level of fidelity without the risk of exposing its operating envelope to adversaries.

Challenge 5

Upgrade, integrate and interoperate at pace

System Update 4. An approach to systems and capability development that reduces the time to market and to introduce upgrades. A modular and evolutionary approach that looks at to unify the best solutions to tackle a changing threat landscape.

Operational Parameters

- Must maintain Sovereign control.
- Must follow a modular design.
- Interoperable with NATO and our Allies.
- Able to adapt to changing problems.

Operational Use Case

Delivery teams across the MOD rely on a modular and evolutionary approach to keep the DTW ahead of shifting threats. NADG maintains the overarching DTW design, aligned with service boundaries defined by CSOC. As new technologies emerge, they can be integrated with minimal disruption, allowing units to adopt upgraded capabilities without extended downtime. Mission owners tailor and combine sovereign components to meet operational needs whilst not affecting over critical functionality. During joint operations, the UK interoperate seamlessly with NATO and allied systems, supporting shared situational awareness and coordinated action. Commanders can draw on the strongest solutions and adapt them rapidly, maintaining operational advantage, ensuring the force remains agile, resilient, and prepared for emerging challenges.

Providing skills, training and tools

Challenge 6

INTEGRATED WARFARE CENTRE

Challenge 6

Providing skills, training and tools

Description. The successful adoption and operation of the DTW require a skilled workforce capable of maximising its value and adapting to its evolution. This necessitates understanding how to access the knowledge and skills required to build and operate a complex and evolving digital system. Addressing this challenge ensures the enterprise is prepared to integrate the DTW into its workflows and has the resources to operate it effectively.

To do this introduces difficulties. Personnel working on these systems are likely to need higher levels of clearances. Any training environments will need emulate the live environment whilst remaining at a lower classification. The training pipeline will need to be updated to reflect the new ways of working. Solutions must be flexible, scalable, and adaptable to incorporate emerging technologies and evolving threats.

Questions to answer.

- How do we train as we fight?
- How do users maintain currency in dynamically changing environment?
- How do we get build the knowledge and skills internally?
- How could this knowledge and skills be drawn more flexibly from the wider UK workforce?
- How do we provide a training environment that reflects the real world?
- How can we use technology to augment the user and reduce the training burden?

Skills & Tools 1. The MOD requires ways of identifying or training people who have an aptitude for working with and developing digital systems from across the current workforce and wider. Ensuring that people are educated and trained to common standards, with common practices and a clear profession. Providing a workforce that have the foundational skills to operate and develop the DTW.

Operational Parameters

- Must look at how we recruit and train new people.
- Must acknowledge the current workforce and how their skills are updated.
- May consider the use of external resources, such as reserves or deployed contractors.

Operational Use Case

The MOD is able to rapidly call upon a broad range people who have the fundamental skills to work in a modern digital environment. It can easily draw these skills from different sources including the existing workforce, reservists, or the wider UK workforce. They have a high level of confidence where these resources are, how to access them and that they possess skills needed to be effectively deployed to task.

Challenge 6

Providing skills, training and tools

Skills & Tools 2. Users need to maintain currency in their training to ensure they are proficient to use the system when required. Any training needs to emulate the live systems accurately as the DTW evolves so users understand the changes before they are using it. The goal is to enable users to train in a realistic way that adequately prepares them to use the tools operationally.

Operational Parameters

- Adaptive training scenarios that simulate realistic, multi-domain targeting scenarios.
- Incorporation of lessons learned from recent conflicts, to ensure training reflects modern threats and operational realities.
- Collaborative training that enables us to practice with NATO partners.
- Simulating contested environments to prepare trainees for high-intensity operations.

Operational Use Case

Users of the DTW can maintain their level of competence, or quickly become proficient again, despite it being an evolving system. Skill fade whilst not using a tool is minimised by design and users who are not permanently deployed using the tool are able to swiftly understand and adapt to the changes. Commanders and system owners are confident that users are capable of operating the system safely and efficiently.

National Armaments
Director Group

Cyber & Specialist
Operations Command