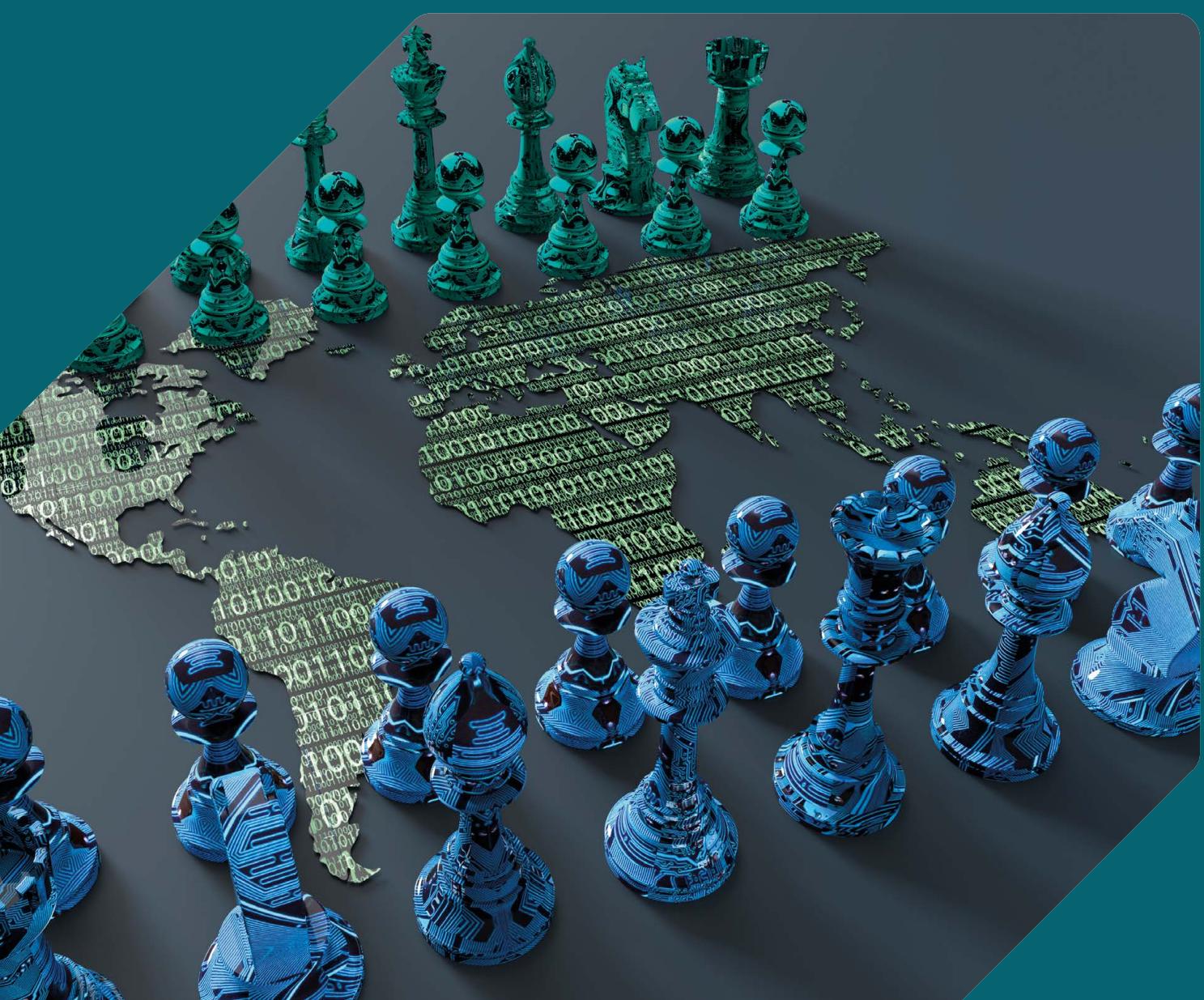




Ministry  
of Defence

# Defence Artificial Intelligence Strategy

June 2022



## **Defence Artificial Intelligence Strategy 2022**

v1.0

June 2022

### **Conditions of Release**

This publication is UK Ministry of Defence (MOD) Crown copyright. Material and information contained in this publication may be reproduced, stored in a retrieval system and transmitted for UK government and MOD use only, except where authority for use by other organisations or individuals has been authorised.

# Foreword by the Secretary of State for Defence



A year ago, we published the Integrated Review, committing to strengthen security and defence and to modernise our armed forces. We warned then that these steps were a necessary response to the deteriorating global security environment, including state-based threats. Since then, Russia's illegal invasion of Ukraine has brought all the horrors of industrial-age warfare back to the heart of Europe. The tragic events unfolding in Ukraine are a stark reminder of the importance of ensuring that our armed forces can meet the sort of conventional military challenge we hoped our continent had left behind in the 20th Century.

However, we also noted that we live in an era of persistent global competition, characterised by hybrid and sub-threshold threats. Russia's appalling invasion of Ukraine removes any blurring of the line between war and peace, but was preceded by many years of malign activity. As we stand in solidarity with the global community in challenging the actions of the Putin regime, we recognise that Defence must be relevant and effective across the spectrum of competition and conflict.

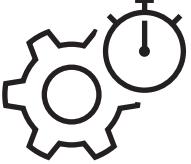
To meet these various challenges, Defence must prioritise research, development and experimentation, maintaining strategic advantage by exploiting innovative concepts and cutting-edge technological advances – and Artificial Intelligence is one of the technologies essential to Defence modernisation. Imagine a soldier on the front line, trained in highly-developed synthetic environments, guided by portable command and control devices analysing and recommending different courses of action, fed by database capturing and processing the latest information from hundreds of small drones capturing thousands of hours of footage. Imagine autonomous resupply systems and combat vehicles, delivering supplies and effects more efficiently without putting our people in danger. Imagine the latest Directed Energy Weapons using lightning-fast target detection algorithms to protect our ships, and the digital backbone which supports all this using AI to identify and defend against cyber threats.

AI has enormous potential to enhance capability, but it is all too often spoken about as a potential threat. AI-enabled systems do indeed pose a threat to our security, in the hands of our adversaries, and it is imperative that we do not cede them a vital advantage. We also recognise that the use of AI in many contexts, and especially by the military, raises profound issues. We take these very seriously – but think for a moment about the number of AI-enabled devices you have at home and ask yourself whether we shouldn't make use of the same technology to defend ourselves and our values. We must be ambitious in our pursuit of strategic and operational advantage through AI, while upholding the standards, values and norms of the society we serve, and demonstrating trustworthiness.

This strategy sets out how we will adopt and exploit AI at pace and scale, transforming Defence into an 'AI ready' organisation and delivering cutting-edge capability; how we will build stronger partnerships with the UK's AI industry; and how we will collaborate internationally to shape global AI developments to promote security, stability and democratic values. It forms a key element of the National AI Strategy and reinforces Defence's place at the heart of Government's drive for strategic advantage through science & technology.

**Rt Hon Ben Wallace MP**

# Defence AI Strategy Overview

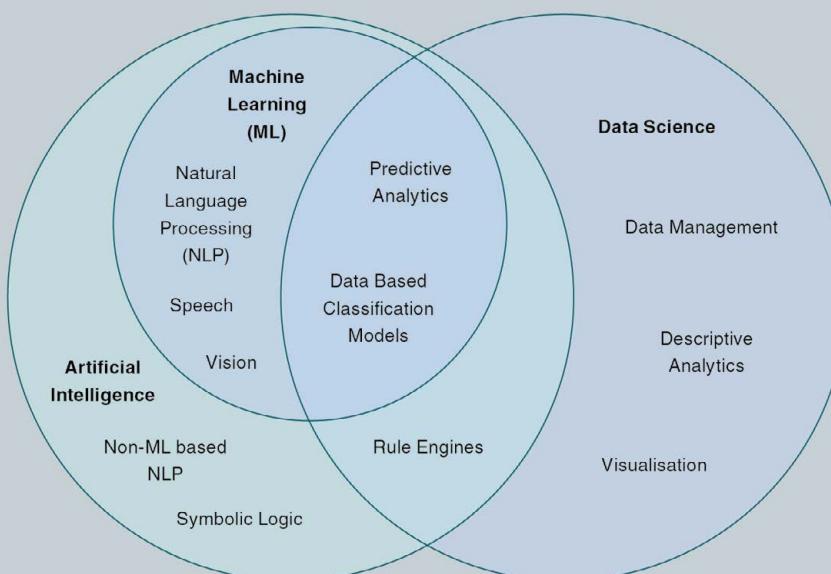
Vision and Approach	<p><b>Our vision is that, in terms of AI, we will be the world's most effective, efficient, trusted and influential Defence organisation for our size.</b></p>			
	<p><b>Objective</b> Transform Defence into an 'AI ready' organisation.</p> <p><b>Actions:</b></p> <ul style="list-style-type: none"><li>• Upskill leaders and workforce, recruit key Talent;</li><li>• Address policy challenges;</li><li>• Modernise digital, data and technology enablers.</li></ul>	<p><b>Objective</b> Adopt and exploit AI at pace and scale for Defence advantage.</p> <p><b>Actions:</b></p> <ul style="list-style-type: none"><li>• Organise for success;</li><li>• Exploit near and longer term opportunities;</li><li>• Systematic experimentation;</li><li>• Collaborate internationally.</li></ul>	<p><b>Objective</b> Strengthen the UK's defence and security AI ecosystem.</p> <p><b>Actions:</b></p> <ul style="list-style-type: none"><li>• Build confidence and clarify requirements;</li><li>• Address commercial barriers;</li><li>• Incentivise engagement and co-creation;</li><li>• Support business growth.</li></ul>	<p><b>Objective</b> Shape global AI developments to promote security, stability and democratic values.</p> <p><b>Actions:</b></p> <ul style="list-style-type: none"><li>• Champion responsible global AI development;</li><li>• Promote security and stability;</li><li>• Develop future security policy.</li></ul>
Outcomes	<p><b>Decision Advantage</b></p> 	<p><b>Efficiency</b></p> 	<p><b>Unlock New Capabilities</b></p> 	<p><b>Empower the Whole Force</b></p> 
Governance	<p>There is no single overall owner for AI in Defence. Every business unit and Function has an important role to play if we are to achieve our goals.</p> <p><b>MOD Head Office</b></p> <ul style="list-style-type: none"><li>• Set AI policy and strategy, define capability targets, direct strategic programmes and ensure overall coherence.</li></ul> <p><b>Business units / Functional Leads</b></p> <ul style="list-style-type: none"><li>• Pursue the forms of AI most relevant to them, guided by this Strategy and direction from Head Office.</li></ul> <p><b>Strategic Command</b></p> <ul style="list-style-type: none"><li>• Ensure strategic and operational integration across the warfighting domains.</li></ul>			
	<p>Overall strategic coherence is managed jointly by the Defence AI and Autonomy Unit (DAU) and the Defence AI Centre (DAIC). The DAU sets strategic policy frameworks governing development, adoption and use of AI. The DAIC is the focal point for AI R&amp;D and technical issues.</p>			

# Contents

<b>Executive Summary .....</b>	<b>5</b>
<b>1. Introduction .....</b>	<b>9</b>
1.1 The Global Technology Context .....	9
1.2 Our Response .....	11
1.3 Ambitious, safe and responsible use of AI .....	13
<b>2. Transform into an ‘AI Ready’ Organisation .....</b>	<b>17</b>
2.1 Culture, Skills and Policies .....	17
2.2 Digital, Data and Technology Enablers .....	22
<b>3. Adopt and Exploit AI at Pace and Scale for Defence Advantage .....</b>	<b>29</b>
3.1 Organising for Success .....	29
3.3 Promoting Pace, Innovation and Experimentation .....	32
3.4 Working Across Government .....	37
3.5 International Capability Collaboration .....	37
<b>4. Strengthen the UK’s Defence and Security AI Ecosystem .....</b>	<b>41</b>
4.1 The UK’s AI Strengths .....	41
4.2 Partnership on the Basis of Trust .....	42
4.3 Clearly Communicating our AI Requirements, Intent and Expectations .....	44
4.4 Addressing Barriers to Frictionless Collaboration .....	46
4.5 Incentivising Engagement and Co-creation .....	47
<b>5. Shape Global AI Developments to Promote Security, Stability and Democratic Values .....</b>	<b>51</b>
5.1 Shape the Global Development of AI in Line with UK Goals and Values .....	53
5.2 Promote Security and Stability .....	54
5.3 Develop Future Security Policy .....	58
<b>6. Strategy Implementation and Beyond .....</b>	<b>61</b>
6.1 Priorities .....	61
6.2 Leadership and Governance .....	63
6.3 Looking Ahead .....	63

# What is Artificial Intelligence?

Defence understands Artificial Intelligence (AI) as a family of general-purpose technologies, any of which may enable machines to perform tasks normally requiring human or biological intelligence, especially when the machines learn from data how to do those tasks.



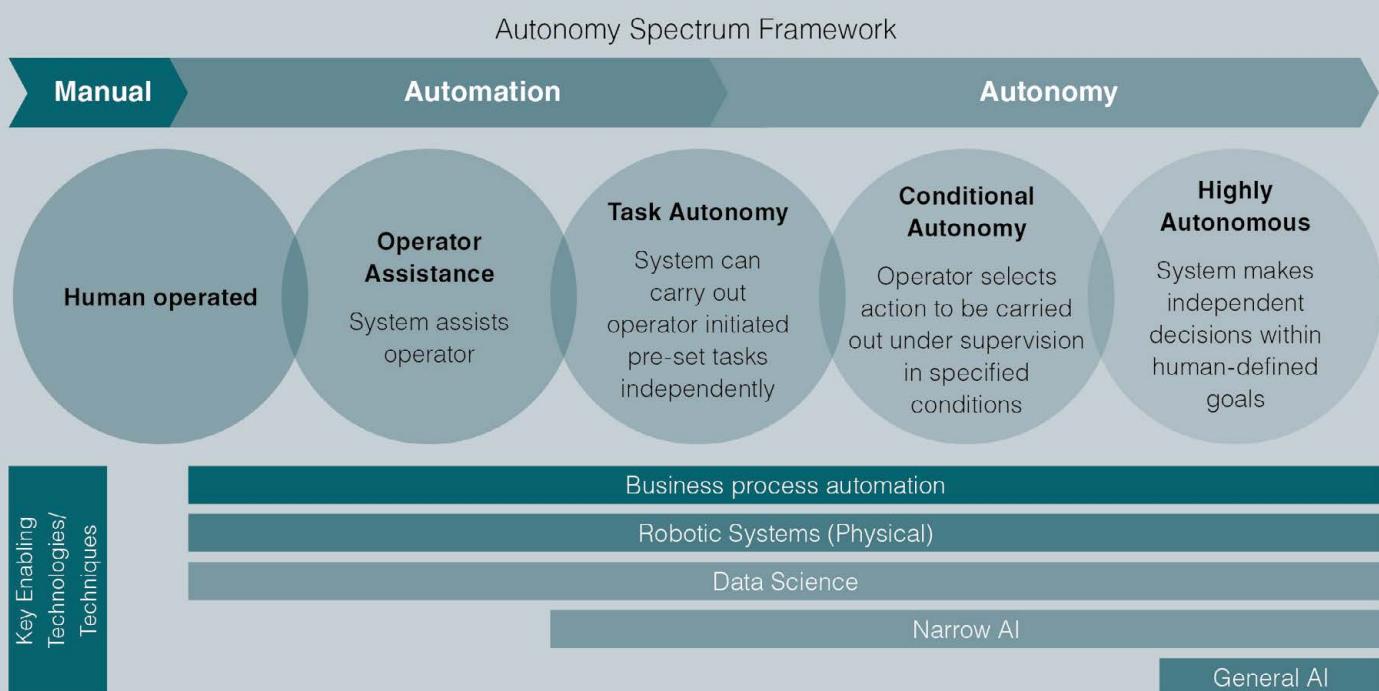
## Overlapping Technologies:

**AI:** Machines that perform tasks normally requiring human intelligence, especially when the machines learn from data how to do those tasks. - *UK National AI Strategy*

**Machine Learning:** Computer algorithms that can 'learn' by finding patterns in sample data and then apply this to new data to produce useful outputs, often using neural networks. - *Alan Turing Institute*

**Data science:** Research that involves the processing of large amounts of data in order to provide insights into real-world problems. - *Alan Turing Institute*

## Levels of Oversight & Control



The appropriate level of human oversight, verification and control will vary depending on the system design, mission objectives and operational context.

# Executive Summary

Our vision is that, in terms of AI, we will be the world's most **effective, efficient, trusted** and **influential** Defence organisation for our size:

**Effective** – through the delivery of battle-winning capability and supporting functions, and in terms of our ability to collaborate and partner with the UK's allies and AI ecosystem;

**Efficient** – through innovative use of technology to deliver capability, conduct operations, and realise productivity benefits across our organisation;

**Trusted** – by the public, our partners and our people, for the safety and reliability of our AI systems, and our clear commitment to lawful and ethical AI use in line with our core values;

**Influential** – in terms of shaping the global development of AI technologies and managing AI-related issues to positive ends, working collaboratively and leading by example.

The **Integrated Review<sup>1</sup>** (2021) highlights national excellence in AI as central to securing the UK's status as a 'Science and Technology Superpower' by 2030. The **National AI Strategy<sup>2</sup>** (2021) notes its huge potential to rewrite the rules of whole industries, drive substantial economic growth and transform all areas of life. The **Integrated Operating Concept<sup>3</sup>** (2020) describes how pervasive information and rapid technological change are transforming the character of warfare. Across the spectrum of military operations, conflict is becoming increasingly complex and dynamic. New technologies generate massive volumes of data, unlock new threats and vulnerabilities and expand the scale of potential attacks through advanced next-generation capabilities (such as swarming drones, high-speed weapons and advanced cyber-attacks).

These technologies – and the operational tempo they enable – are likely to compress decision times dramatically, tax the limits of human understanding and often require responses at machine speed.

As the **Defence Command Paper<sup>4</sup>** (2021) notes, "future conflicts may be won or lost on the speed and efficacy of the AI solutions employed".

Simultaneously, information operations are increasingly important to counter false narratives that distract attention, provide cover for malign activities and undermine public support. In short, **a radical upheaval in defence is underway and AI-related strategic competition is intensifying**. Our response must be rapid, ambitious, and comprehensive.

**This strategy sets out how we will approach this significant strategic challenge.** It should be read by all senior leaders in Defence and cascaded widely throughout the organisation **because AI affects everybody.** It has particular relevance to all those involved in Defence Force Development and Defence Transformation, whose structures and processes will have a key role to play in implementation and delivery – but **every part of Defence must identify those elements relevant to them and act accordingly.**

We must **transform into an ‘AI ready’ organisation.** We will proactively drive changes to our culture, skills and policies, training leaders, upskilling the workforce, and strengthening the Defence AI & Autonomy Unit. We will create a **Defence AI Skills Framework** and new AI career development and progression pathways. We will recognise that data is a critical strategic asset, curating and exploiting it accordingly. We will

implement the **Digital Strategy for Defence<sup>5</sup>** (2021) and the **Data Strategy for Defence<sup>6</sup>** (2021), and deliver a new **Digital Backbone** and **Defence AI Centre.** Some elements of this transformation (especially Digital and Data enablers) will be delivered or supported on a pan-Defence basis, guided by a new **AI Technical Strategy**, but this is a challenge for every part of our organisation with the nature of that challenge depending on the specific organisation, its business, and the opportunities provided by AI.

We must **adopt and exploit AI at pace and scale for Defence advantage**, establishing AI as one of our top priorities and a key source of strategic advantage within our Capability Strategies and Force Development processes. Our opportunity and our challenge lie in the sheer breadth of AI applications across our organisation. In the near term, we will enhance our effectiveness, efficiency and productivity through the systematic roll-out

## Priority Outcomes through AI

By meeting the objectives of this Strategy, and through the adoption of AI-enabled technologies our Armed Forces will modernise and rapidly transition from an industrial age Joint Force into an agile Information Age Integrated Force. The Defence organisation will also benefit from increased efficiency and productivity. The priority outcomes we currently understand and expect to see are summarised below.



### Decision Advantage

Increase operational tempo and agility through better-informed and distributed decision-making and machine-speed responses to threats.



### Efficiency

Improve flexibility, productivity and availability through intelligent automation.



### Unlock New Capabilities

Secure operational advantage by developing novel ways to operate, deliver enhanced military effect and protect our people from harm.



### Empower the Whole Force

Reduce burdens and focus human talents on higher value functions requiring ingenuity, contextual thinking and judgement.

and adoption of '**AI Now**': mature data science, machine learning and advanced computational statistics techniques. In parallel, we will invest in '**AI Next**': cutting-edge AI research and development integrated within our broader R&D pipelines. **Integrated multi-disciplinary delivery**

**teams** will be at the heart of our approach to AI adoption and the development of effective **Human-Machine Teaming**, combining human cognition, inventiveness and responsibility with machine-speed analytical capabilities. We will establish a centre to assess and mitigate AI system vulnerabilities and threats. We will work closely with allies and partners, developing innovative capability solutions to address common challenges, while sharing the burdens of maintaining niche yet essential AI development and test capabilities.

We must **stimulate and support the UK's defence and security AI ecosystem<sup>7</sup>**, building on commitments set out in the **Defence & Security Industrial Strategy<sup>8</sup>** (2021) and the **National AI Strategy**. Our ability to exploit these technologies is rooted in the vitality of our industrial and academic AI base. We will champion and support our national AI ecosystem **as a strategic asset in its own right**, forging a more dynamic and integrated partnership. We will foster closer links with the sector, establishing a new **Defence & National Security AI Network**, promoting talent exchange and co-creation, communicating a scaled demand signal to encourage civil sector investment in defence-relevant AI R&D, and simplifying access to Defence data and assets. We will continue to **improve our acquisition system** to drive greater pace and agility in delivery. We will

also take steps to promote opportunities for small & medium-sized enterprises, modernise regulatory approaches and maximise the exploitation and commercialisation of Defence-held AI-related intellectual property. We will do all of this within Defence whilst more broadly supporting the transition to an AI-enabled economy, capturing the benefits of innovation in the UK.

We must **shape global AI developments to promote security, stability and democratic values**. As AI becomes increasingly pervasive, it will significantly alter global security dynamics. It will be a key focus for geostrategic competition, not only as a means for technological and commercial advantage but also as a battleground for competing ideologies. We will shape the development of AI in line with UK goals and values, promoting ethical approaches and influencing global norms and standards, in line with democratic values. We will promote security and stability, ensuring UK technological advances are appropriately protected, countering harmful technology proliferation and exploring mechanisms to build confidence and minimise risks associated with military AI use. As we develop our security policies to reflect AI-related challenges we will maintain a broad perspective on implications and threats, considering extreme and even existential risks which may arise, and engaging proactively with allies and partners. We will champion strategic risk reduction and seek to create dialogue to reduce the risk of strategic error, misinterpretation and miscalculation. We will ensure that – regardless of any use of AI in our strategic systems – human political control of our nuclear weapons is maintained at all times.



Madfox Autonomous Surface Vehicle

# 1. Introduction

We face a strategic imperative: adapt and excel in our exploitation of technologies like Artificial Intelligence (AI), or increasingly fall behind our allies and competitors. The challenges are far-reaching and fundamental, and we must be ambitious.

## 1.1 The Global Technology Context

The Integrated Review identifies rapid technological change as a critical strategic challenge. New technologies are being developed and adopted faster than ever before, driving profound changes across our societies, politics and economies, and accelerating the emergence of threats. While break-through discoveries are driven by Government and universities, industry and commercial opportunities are key engines of innovation. Global competition for rare talent is fierce. Technology is an arena of intensifying and increasingly critical competition between states, both in prosperity and security terms and as an expression of different visions for society.

Adversaries are investing heavily to challenge our technological edge and threaten our interests. Increasingly, we are seeing hostile acts against our societies, economies and democracies that are difficult to detect, complex to challenge, and more difficult still to deter. **Our future security, resilience, international standing and prosperity will be defined by our ability to comprehend, harness and adapt to rapid technological change.**

### 1.1.1 The Significance of Artificial Intelligence

AI is perhaps the most transformative, ubiquitous and disruptive new technology with huge potential to rewrite the rules of entire industries, drive substantial economic growth and transform all areas of society. It will be part of most future products and services, powering the 4<sup>th</sup> Industrial Revolution and affecting every aspect of our lives. This Strategy defines AI as a family of general-purpose technologies, any of which may enable machines to perform tasks that would traditionally require human or biological intelligence, especially when the machines learn from data how to do those tasks; for example, recognising patterns, learning from experiences, making predictions and enabling actions to be taken.

Defence applications for AI stretch from the corporate or business space - the 'back office' - to the frontline: helping enhance the speed and efficiency of business processes and support functions; increasing the quality of decision-making and tempo of operations; improving the security and resilience of inter-connected networks; enhancing the mass, persistence, reach and effectiveness of our military forces; and protecting our people from harm by automating 'dull, dirty and dangerous' tasks.



## Exercise SPRING STORM – AI on the Ground

In May 2021, AI was used on a British Army operation for the first time. Soldiers from the 20th Armoured Infantry Brigade trialled a Machine Learning engine designed to process masses of complex data, including information on the surrounding environment and terrain, offering a significant reduction in planning time over the human team; whilst still producing results of equal or higher quality.

The trial demonstrated the potential for AI to quickly process vast quantities of data, providing commanders with better information during critical operations and transferring the cognitive burden of processing data from a human to a machine. The Machine Learning engine had been developed in partnership with industry and used automation and smart analytics along with supervised learning algorithms. This AI capability can be hosted in the cloud or operate in independent mode. By saving significant time and effort, it provides soldiers with instant planning support.

This is one of the first steps towards achieving machine-speed command and control. The trial took place during an annual large-scale exercise with soldiers from NATO's Enhanced Forward Presence Battlegroup, led by the British Army.

**Above:** UK personnel participating in exercise SPRING STORM, with other NATO allies in Estonia

The potential to supplement or replace human intelligence raises fundamental questions about our relationship with technology, the personal and societal implications of big data, and the scope for human agency, rights and accountability in an age of data-driven, machine-speed decision-making. Nevertheless, the widespread use and adoption of these technologies is irresistible – those who adopt and adapt successfully will prosper; the unsuccessful will fall behind. Realising the benefits of AI – and countering the resulting threats – may be one of the most critical strategic challenges of our time.

The UK will lead by example, working with partners around the world to make sure international agreements embed our ethical values, and making clear that progress in AI must be achieved responsibly and safely, according to democratic norms and the rule of law.

## 1.1.2 AI Threats

The use of AI by adversaries will heighten threats above and below the threshold of armed conflict. AI has potential to enhance both high-end military capabilities and simpler low-cost ‘commercial’ products available to a wide range of state and non-state actors. Adversaries are seeking to employ AI across the spectrum of military capabilities, including offensive and defensive cyber, remote and autonomous systems, situational awareness, mission planning and targeting, operational analysis and wargaming and for military decision support at tactical, operational and strategic levels.

Adversary appetite for risk suggests they are likely to use AI in ways that we would consider unacceptable on legal, ethical or safety grounds. Equally, adversaries will use a range of information, cyber and physical means to attack our AI systems and undermine confidence in their performance, safety and reliability (e.g. by ‘poisoning’ our data, corrupting hardware components in our supply chain, or interfering with communications and commands).

## 1.1.3 AI Competition

Global competition for advantage through AI is intense. Allies, adversaries and systemic competitors are investing heavily to develop research capabilities, maximise access to talent and accelerate solutions to market. The UK has significant strengths and is recognised as an AI powerhouse. Our thriving AI sector is worth over £15.6bn<sup>9</sup> and ranked amongst the most innovative and productive in the world. Our vibrant digital sector – worth £149bn in 2018<sup>10</sup> – creates innovative businesses, produces ‘unicorns’<sup>11</sup> and employs highly skilled people across the UK, with the 3rd highest number of AI companies in the world. While the US is the current world leader in AI technologies (e.g. in research and patents; in government and private sector investment<sup>12</sup>; and in the range, reach and size of their AI industrial base), China has substantially accelerated the development of its own AI ecosystem to become world class in many aspects, including the development of AI Talent<sup>13</sup>. Dozens of countries have published ambitious AI strategies to secure economic, societal and security benefits. This offers great scope for collaboration, though opportunities must be balanced against national security risks.

## 1.2 Our Response

**We are well-placed to take advantage of AI opportunities by capitalising on our national R&D strengths**, aligning with the broader aims set out in the **National AI Strategy** to promote long-term investment and planning, support the transition to an AI-enabled economy and optimise national and international governance. Over 200 AI-related R&D programmes are underway in Defence, ranging from machine learning applications to ‘generation after next’ research; and covering areas from autonomous ships and swarming drones, to talent management and predictive maintenance.

# Understanding the Threat

Adversaries and systemic competitors are investing heavily in AI technologies to challenge our defence and security edge. We have already seen claims that current conflicts have been used as test beds for AI-enabled autonomous systems, and we know that adversaries will use technology in ways that we would consider unethical and unsafe.

Potential threats include enhanced Cyber and information warfare, AI-enabled surveillance and population control, accelerated military operations and the use of autonomous physical systems. Non-state actors are seeking to weaponise advanced commercial products to spread terror and hold our forces at risk. As these case studies illustrate, this is not a hypothetical future but the here and now.

As Hostile State and Non-State Actors build their AI capabilities, they will increasingly attempt to acquire key technologies and Intellectual Property from UK academia and Industry. This is a major threat. The UK must prepare to defend our most valuable technologies and capabilities, protect our universities from foreign interference, and safeguard industry, intervening where necessary.



© UAC



© File Image via Saudi Forces

## State-Based Threats

Adversaries are developing military AI and AI-enabled robotic systems in pursuit of information superiority and capability advantage.

Open-source analysis<sup>FN</sup> suggests Russia is prioritising AI R&D in areas such as Command and Control, Electronic Warfare, Cyber, and uncrewed systems in all domains.

One example is the S-70 Okhotnik: a 25 ton, jet powered unmanned combat air system with stealth features to help it survive in contested airspace. Russia claims it has a level of artificial intelligence and that missions may include ISR, Electronic Warfare and air-to-surface / air-to-air strike. Flight testing commenced in 2019 and is on-going, with claims it will enter into service as soon as 2025<sup>1</sup>.

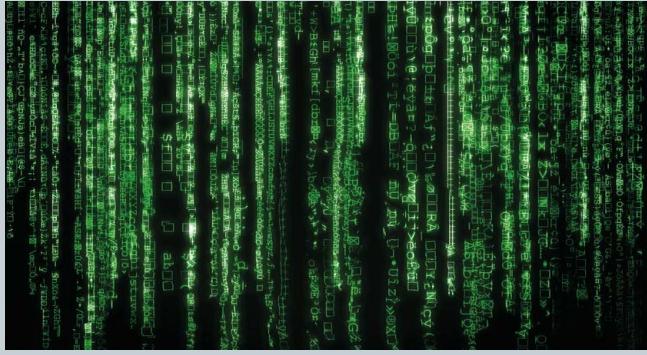
## Advanced ‘Proxy’ Threats

Non-state actors are repurposing commercial technologies to enhance their capabilities.

For example, in 2017 Iranian-backed Houthi forces in the Yemen used an Uncrewed Surface Vehicle (USV; probably a converted fishing skiff) loaded with explosives to severely damage the Saudi Arabian naval frigate, AL-MADINAH. They have since used USVs to attack maritime targets at up to 1000km and also launched attacks using Uncrewed Air Vehicles (likely with support from Iran).

While current systems may be limited to GPS waypoint navigation to reach a predetermined target, irresponsible proliferation of AI technologies could enable proxies to field far more dangerous capabilities in future.

[1] [www.chathamhouse.org/2021/09/advanced-military-technology-russia/06-military-applications-artificial-intelligence](http://www.chathamhouse.org/2021/09/advanced-military-technology-russia/06-military-applications-artificial-intelligence)



## AI-Enhanced Cyber Threats

Artificial Intelligence has the potential to significantly increase the impact of malicious cyber attacks, potentially probing for and exploiting cyber vulnerabilities at a speed and scale that is impossible for human monitored systems to defend against.

AI could also be used to intensify information operations, disinformation campaigns and fake news, for example through broad spectrum media campaigns or by targeting individuals using bogus social media accounts and video deep fakes.

## Other AI Threats

AI is increasingly being used by adversaries across the full spectrum of military capabilities, including for situational awareness, optimised logistics, operational analysis and wargaming and for decision support at tactical, operational and strategic levels.

Hostile states are almost certainly conducting research in the use of AI for mission planning and targeting, building on capabilities that are already used to curtail civil liberties, e.g. CCTV surveillance and online monitoring.

This is a promising start, but a step change is urgently required if we are to embrace AI at the pace and scale required to match the evolving threat. This Strategy sets out a comprehensive response to the opportunities and disruptive impacts of AI, along with the short to medium term actions that we will take to address these challenges and catalyse a once-in-a-generation technological shift across every part of our business, in our operational activities and in our partnerships.

Our objectives are to:

- **Transform into an ‘AI ready’ organisation**, investing in critical enablers and shaping a culture fit for the Information Age;
- **Adopt and exploit AI at pace and scale for Defence advantage**, pursuing both ambitious, complex projects and simpler, iterative approaches;
- **Strengthen the UK’s defence and security AI ecosystem**, recognising the fundamental need to work with partners across government, industry and academia;
- **Shape global AI developments to promote security, stability and democratic values**, projecting influence internationally and working with allies.

## 1.3 Ambitious, safe and responsible use of AI

AI has extraordinary potential as a general enabling technology. We intend to realise its benefits right across our organisation, from ‘back office’ to battlespace. We particularly seek to deliver and operate world-class AI-enabled systems and platforms, including AI-enabled weapon systems.



Royal Navy innovation experts NavyX and industry partners BAE Systems saw the Type 23 frigate HMS Argyll take command of an uncrewed Pacific 24 rigid inflatable boat (RIB) while sailing at sea.

**However, we recognise that the use of AI in many contexts – and especially by the military – raises profound issues. There are concerns about fairness, bias, reliability, and the nature of human responsibility and accountability.**

(For example, there are well documented instances of recruiting software demonstrating racial or gender bias). Unintended or unexpected AI-enabled outcomes could clearly have particularly significant consequences in an operational context. **We take all these issues very seriously.**

### 1.3.1 Our commitment as a responsible AI user

The **National AI Strategy** states that the UK public sector will lead the way by setting an example for the safe and ethical deployment of AI through

how it governs its own use of the technology. As we pursue strategic and operational advantage through AI, **we are determined to uphold the standards, values and norms of the society we serve, and to demonstrate trustworthiness.**

**We have therefore published details of our approach, which will be ‘Ambitious, Safe, Responsible’<sup>14</sup>. UK military capabilities and operations will always comply with our national and international obligations.** We will maintain rigorous and robust safety processes and standards by ensuring our existing approaches to safety and regulation across Defence are applied to AI. Our approach applies however and wherever in Defence AI is used, throughout system lifecycles, and is guided by robust ethical principles, developed in collaboration with the Centre for Data Ethics and Innovation (CDEI)<sup>15</sup>. As well as providing a blueprint for responsible

AI, this approach is also the best way of ensuring fast-paced, effective and innovative AI adoption – giving our people and our partners across Industry and Academia (including bodies such as the AI Council, Turing Institute, and the Trustworthy-Autonomous Systems Hub) the confidence to develop concepts, techniques and capability, meeting our operational needs, and reflecting deeply-held values.

## 1.3.2 Our commitment to our people

Our pursuit of AI-enabled capabilities will not change our view that **our people are our finest asset**. AI has tremendous power to enhance and support their work (e.g. enabling analysts to make sense of ever greater quantities of data), but we understand that some challenges require human creativity and contextual thinking, and that the real-world impact of military action demands applied human judgement and accountability. We will not

simplistically assume that AI inherently reduces workforce requirements, even if it does change the activities we need people to undertake. Where staff are affected by the adoption of AI, we will support them and help them find new roles and skills.

We recognise we should use AI to minimise the risks faced by our people. As part of our approach to responsible AI, we also recognise the importance of not exposing our people to legal jeopardy in the operation of novel technologies.

Machines are good at *doing things right* (e.g. quickly processing large data sets). People are good at doing the *right things* (e.g. evaluating complex, incomplete, rapidly changing information guided by values such as fairness). **Human-Machine Teaming will therefore be our default approach to AI adoption**, both for ethical and legal reasons and to realise the ‘multiplier effect’ that comes from combining human cognition and inventiveness with machine-speed analytical capabilities.



HORIBA MIRA VIKING multirole Uncrewed Ground Vehicle

# 2. Transform into an ‘AI Ready’ Organisation

Defence must rapidly transition from an industrial age Joint Force into an agile, Information Age Integrated Force to stay ahead of adversaries amid an increasingly complex and dynamic threat environment. Rapid and systematic adoption of AI – where it is the **right** solution – will be an essential element in realising this ambition.

This Chapter sets out the foundational ‘enablers’ that are urgently needed to properly prepare Defence for widespread AI adoption. **All organisations and Functions will need to address their ‘AI readiness’** – with key elements and support provided across Defence by Functional Owners (particularly Digital) – based on the following approach:

1. Have you assessed how AI will shape the future of your business or function? Have you identified those areas where AI is the **right** solution?
2. Do you have the right culture, leadership models, policies and skills to act rapidly on AI-driven outputs?
3. Do you have accessible, structured, exploitable data? Are you continually collecting data?
4. Do you have access to appropriate scalable computing power (with cloud and ‘edge’ computing as required)?

5. Do you have models? Are they fit for purpose and can you build, test, deploy and update them quickly enough?

## 2.1 Culture, Skills and Policies

Our internal systems and processes have often failed to keep pace with those used to drive digital transformation in the private sector. We must change into a **software-intensive enterprise**, organised and motivated to value and harness data, prepared to tolerate increased risk, learn by doing and rapidly reorient to pursue successes and efficiencies. **We must be able to develop, test and deploy new algorithms faster than our adversaries.** We must be agile and integrated, able to identify and interpret threats at machine speed with the **cross-domain culture** necessary to defend, exploit, respond and recover in real time.

This is a whole-of-Defence challenge, within the context of a national AI skills gap. We must raise understanding of AI at all levels: ensuring

leaders can navigate the hype, seize opportunities and act as smart ‘customers’ and champions of AI services; improving AI literacy across our professional communities (particularly among policy, legal and commercial staff); growing expertise in deep AI coding and engineering skills across the Whole Force, including with our partners in industry; and generating an informed user-base with the knowledge and confidence to use new capabilities effectively. We will increase the diversity of people working with and developing AI, to best reflect and protect society.

The **National AI Strategy** sets out the Government’s interventions, focusing on three areas to attract and train the best people: those who build AI, those who use AI (OAI<sup>16</sup>), and those we want to be inspired by AI. We will work with the Office for AI and colleagues across Government, tapping into these national programmes where appropriate, including programmes to allow greater flexibility and mobility of global AI talent, to ensure Defence remains at the forefront of AI development and deployment.

## 2.1.1 Strategic Planning for Defence AI skills

Our ability to deliver critically depends on our ability to develop, attract and retain skilled people across Defence. However, the global marketplace for AI talent is intense and Defence risks a severe skills deficit if we do not act quickly and decisively. We must understand our AI skills requirements across the board, modernise our recruitment and retention offer and act strategically to ensure we have the right people in the right places to deliver. We will:

- Develop a whole-force **Defence AI Skills Framework**, aligned to the Pan Defence Skills Framework, identifying skills requirements across Defence as every organisation will need a mix of AI skills suitable to its activities;

- Identify and unlock **policy barriers** so that we can recruit the right talent and skills, developing options for an **AI pay premium** to incentivise recruitment, upskilling and retention, and exploring **flexible ways of recruiting elite talent**, including lateral entry;
- Set benchmarks for recruitment and retention against key categories, actively **monitoring AI workforce ‘pinch points’** and providing assurance on the deliverability of local plans and sustainability of critical capabilities.

## 2.1.2 Applying the Brightest Minds to the AI challenge

Effective multi-disciplinary AI development and delivery teams require a range of specialists, including data scientists, AI developers, machine learning engineers and AI analysts. An AI career in Defence must be recognised as an attractive, aspirational choice for this highly skilled talent. In parallel, we must make the most of our existing people, identifying and developing individuals that have the aptitude and attitude for AI careers. We will:

- Establish a **Head of AI Profession** (sitting within the Defence AI Centre (DAIC), described in section 2.2.3) responsible for the AI Skills Framework, developing our recruitment and development retention offer, setting standards for delivery team skills (particularly for new or novel deployments of AI) – working with the Defence Digital, Data and Technology (DDaT<sup>17</sup>) and Cyber Professions, FLCs, CDP and the Government Digital Service;
- Create **AI career development and progression pathways** – owned by the Head of AI Profession – with options for deep specialists as well as skilled generalists. This will build on existing ‘best in class’ initiatives in Defence (e.g. Jhub coding training) and wider government (e.g. the Data Science Accelerator);



An **X2 Uncrewed Ground Vehicle (UGV)** on display at a capabilities demonstration at AWE20.

- Develop new mechanisms to **identify and incubate AI talent within Defence**, potentially including aptitude testing, flexible entry paths to the new AI profession and incentive schemes to encourage uptake of advanced technical courses;
- Explore options for **Unified Career Management** of military AI professionals, similar to the model that has been established for Cyber professionals. AI awareness and understanding should be incorporated within military training syllabuses and we will examine options for a dedicated AI Academy as part of the Defence Academy;
- Strengthen existing academic partnerships and explore options to tap into government supported interventions across **top talent**,

**PhDs and Masters levels.** This includes **Turing Fellowships, Centres for Doctoral Training, Postgraduate Industrial-Funded Masters** and **AI Conversion Courses**. We will examine placement schemes for **AI Masters students** to gain practical experience in Defence, and work with national skills programmes to increase the volume of UK talent in critical areas;

- Use more **specialist reservists**, tailoring recruitment exercises to attract data-literate individuals to ensure we make effective use of the UK's wider AI talent pool – an essential component of the Whole Force.

## 2.1.3 AI Leadership at All Levels

Lack of understanding cannot be a barrier to AI exploitation. Leaders at all levels must be equipped to appreciate the benefits AI can provide, the risks they need to look out for, and any ethical and societal implications that might arise (with technical knowledge varying by roles). We will:

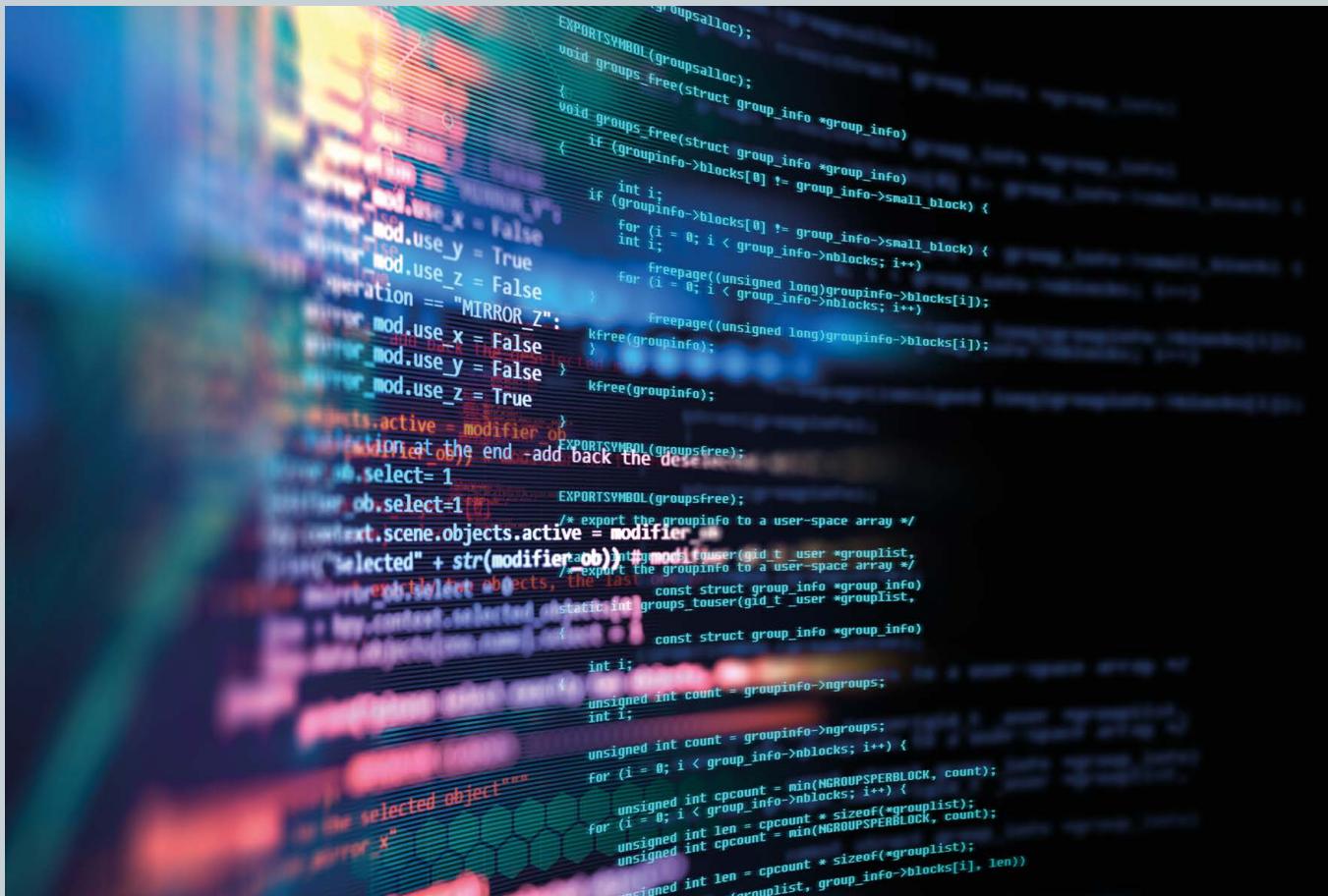
- Mandate that **all senior leaders across Defence** must have foundational and strategic understanding of AI and the implications for their organisation;
- Provide **targeted products to engage and support “middle level” leaders** ensuring they have the training and understanding necessary to identify and exploit AI-enabled opportunities and manage implementation risks;
- Support leaders at all levels through coherent **AI leadership training programmes**, including appropriate horizon scanning products and communities of interest to share understanding of issues, opportunities and best practice;
- Task all Defence organisations and Functions to review policies and processes to ensure leaders are **empowered** to seize AI opportunities at pace;
- Establish an **Engagement and Interchange Function**, delivered by the Defence AI Centre, to encourage seamless interchange between Defence, academia and the tech sector. Working with academia and industry (including the AI Council, the Alan Turing Institute and the Defence Growth Partnership SME forum), we will use secondments and placements to **bring in talented AI leaders from the private sector** with a remit to conduct high-risk innovation and drive cultural change; **create opportunities for external experts**

**to support policy-making; and develop schemes for Defence leaders to gain tech sector experience.** We will ensure our approach works for both SMEs as well as our more familiar defence partners.

## 2.1.4 Upskilling our Workforce

We will generate an informed community of AI users across our workforce, enshrining an understanding of AI and Data as a fundamental component of professional development at all levels of the organisation, supported by appropriate training and awareness. In addition to general digital literacy, our people must have enough understanding to work confidently, effectively and responsibly with AI tools and systems. We need AI experts from a range of diverse backgrounds across all the professions; from policy and legal to commercial expertise. This is particularly important in the context of military operators, so we will:

- Explore options to establish and manage a distinctive ‘AI-enabled military operator’ skill-set or trade, adapting existing skill-sets where AI becomes a significant factor;
- Institute clear and auditable processes for the licensing and routine re-certification of military AI operators, akin to licences to operate vehicles or machinery, where appropriate;
- Integrate AI and Human Machine Teaming throughout our training and exercise programmes, using real, virtual and simulated techniques, and establish clear systems to capture and learn AI-related lessons from our operational deployments.



## Military Data Science skills

Defence Intelligence's Military Data Science programme has trained personnel in coding and basic data science techniques. Service personnel complete postgraduate Data Science training, receive mentoring from experts and have access to data and development environments. This programme provides a deployable capability that can straddle knowledge of operations, intelligence, and data science. Military Data Science have been able to utilise open-source AI algorithms to provide information advantage to a wide range of intelligence operational requirements, including ensuring that data-centric intelligence is delivered at pace whilst on operations. This has led to the delivery of data science projects where a deep understanding of intelligence and operations, blended with an appreciation of data science techniques, has allowed significant contributions to intelligence analysts' work.



## 2.1.5 Diversity and Inclusion

We are committed to increasing the diversity and inclusivity of our workforce. It is right that we represent the communities we serve, and diversity & inclusion promotes creativity, brings novel perspectives to bear and helps challenge established or outdated approaches. Our skills interventions will strengthen the diversity and inclusiveness of our workforce.

These qualities are particularly important in the development and exploitation of new technologies, helping us imagine and develop novel capabilities and tactics, avoid strategic surprises, and anticipate unintended consequences. Diverse & inclusive design, development and operational teams are essential to understand how AI systems affect and are usable by different personnel, and to mitigate biases and other effects which may otherwise pass unnoticed while disproportionately impacting certain groups.

We also recognise that – used properly – AI may be a powerful tool to help promote diversity. Diversity & inclusion principles will therefore underline all elements of this strategy; further, we will continuously assess diversity & inclusion in the development and deployment of AI and act where needed to improve it.

## 2.1.6 Policy, Process and Legislation

The **MOD Science & Technology Strategy**<sup>18</sup> (2020) highlights the importance of ‘anticipatory policy making’ – resolving policy issues before the point of technology maturation – for the successful adoption of new capabilities. The **Defence AI & Autonomy Unit (DAU)** was created in 2018 to help the department adopt these technologies at pace. We must now accelerate efforts to ensure our policies, processes and approaches to legislation

enable, rather than constrain us. As examples: HR policies will need to be updated to ensure that staff can use AI effectively and fairly to speed up recruitment; our ability to glean crucial insights from ever-greater quantities of data depends on the intellectual property and commercial frameworks which underpin procurement.

Effective adoption of AI also hinges on questions about existing intelligence-related legislation and information-sharing permissions; and the planning and conduct of military operations involving AI-enabled capability will be shaped by policies governing factors such as the delegation of command & control. We will therefore:

- **Strengthen the DAU** as our focal point for AI-related policy and strategic coherence. Functional Owners and policy leads across Defence will work with the DAU to ensure policies and processes align with this Strategy, and to identify and address priority issues;
- Establish a multi-disciplinary ‘**Operational AI**’ task force to focus particular effort on AI policy issues affecting national or coalition military operations and key intelligence activities;
- Work with the Office for AI and colleagues across Government to identify and address key **cross-cutting policy or legal considerations** to support timely Defence adoption of AI.

## 2.2 Digital, Data and Technology Enablers

Advantage in AI will depend on our ability to provide battle-winning algorithms and trusted machine-ready data to those that need it, when they need it, regardless of geography, platform or organisational boundaries. The right digital, data and technological enablers will be essential.



## Expeditionary Robotics Centre of Expertise (ERCoE)

The Expeditionary Robotics Centre of Expertise (ERCoE) brings together robotics and autonomous systems experts from across MOD, academia and industry with a collaborative and agile-by-design approach. Examples of autonomy projects include:

**Nano Uncrewed Air Systems** are small, autonomous drones designed for use in the field. Usually weighing less than 200 grams and featuring high-quality full motion video cameras and thermal imaging capabilities. An autopilot system enables the operator to handle the UAV in two modes – direct control or autonomously, following a predefined path. These autonomous vehicles can provide ‘eyes on’ around obstacles such as corners and walls, and increased awareness in harsh and challenging conditions, including over terrain.

### Robotic Platoon Vehicles (RPV) and ATLAS

#### (Autonomous Ground Vehicle Projects)

use Machine Learning neural networks to analyse aerial and 3D imagery, classifying the traversability of terrain (e.g. dense woodland – poor, roads – good), to enable the systems to automatically generate and travel along routes. Machine Learning is also used to analyse camera data and identify objects in the environment that the vehicles might need to avoid or stop for. These objects could be humans, vehicles or plants. In the case of ATLAS, camera data is also used to identify features in the environment which, with other sensor data, allow the vehicle to navigate without the need for GPS.



## 2.2.1 Trusted, Coherent and Reliable Data

**Data is a critical strategic asset, second only to our people in terms of importance.** In recognition of this the Defence data transformation is underway with a central Data Office established within Defence Digital, as well as a **Defence Data Framework**<sup>19</sup> (2021) to transform Defence's culture, behaviour and data capabilities.

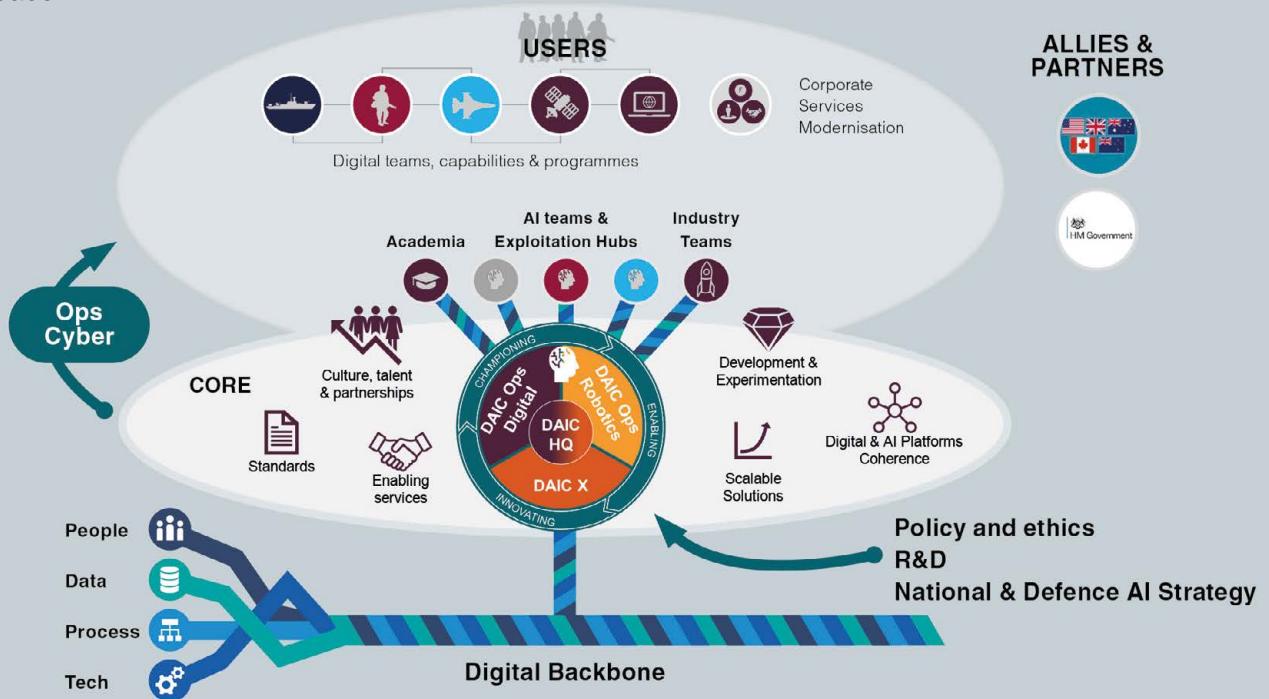
There remains much to do, however, as our vast data resources are too often stove-piped, badly curated, undervalued and even discarded.

We have published the **Digital Strategy for Defence** and the **Data Strategy for Defence** which set out how we will transform into a data-driven organisation: breaking down digital silos; establishing common data architectures, standards, labelling conventions and exploitation platforms (including an operational AI Analytics Environment); and driving appropriate access to integrated, curated and validated data across the Defence enterprise. Building on these measures, the priority of *this* Strategy is that data *is* exploited. We will:

- **Maintain data strategies** within each part of our organisation, identifying what data will be a key source of advantage or efficiency, and how

## Defence AI Centre Architecture

The Defence Artificial Intelligence Centre (DAIC), a part of the Digital Foundry, is an enabling and delivery unit that will unleash the power of Defence's data and allow development and exploitation of AI at scale and pace.



The DAIC will accelerate adoption and scale the impact of AI across Defence through:

- ✓ **CHAMPIONING** by acting as a visionary hub, championing AI development and use across Defence
- ✓ **INNOVATING** by rapidly developing, delivering and scaling AI projects that generate breakthroughs in strategic advantage
- ✓ **ENABLING** by providing common AI services, best practice and a critical mass of expertise to support local adoption across Defence

- it will be obtained or captured. ‘Data registers’ will be available across MOD to promote experimentation and interoperability;
- Embrace new ways to collect AI-relevant data, including by requiring software products and services to be instrumented to generate use and performance data (taking care not to impinge on people’s autonomy, privacy and rights);
  - Adopt new processes and ways of working (including suitable templates, formats and standards) to generate the structured data which can be effectively exploited downstream;
  - Embed protocols to ensure the veracity and integrity of our data sets, including that obtained from external (and possibly open) sources, and to **mitigate risks of bias**;
  - Review data-sharing arrangements with allies, industry and academia, including by exploring innovative ways to **streamline data-sharing bureaucracy** and introducing measures that ensure data shared with or generated by partners remains **accessible** to Defence;
  - Develop security protocols that encourage positive risk-taking while effectively protecting our data from adversarial attack and manipulation. This includes **declassification and permissions** mechanisms to encourage data sharing with fast-moving AI developers.

## 2.2.2 Computing Power, Networks and Hardware

Fast, scalable and secure compute power and seamless network infrastructures are critical to fully exploit AI across Defence - enabling data to flow seamlessly across sensors, effectors and decision makers, so it can be exploited for strategic military advantage in the battlespace and to drive efficiencies in the business space. The Digital Strategy for Defence sets out how this will be delivered through the **‘Digital Backbone’**,

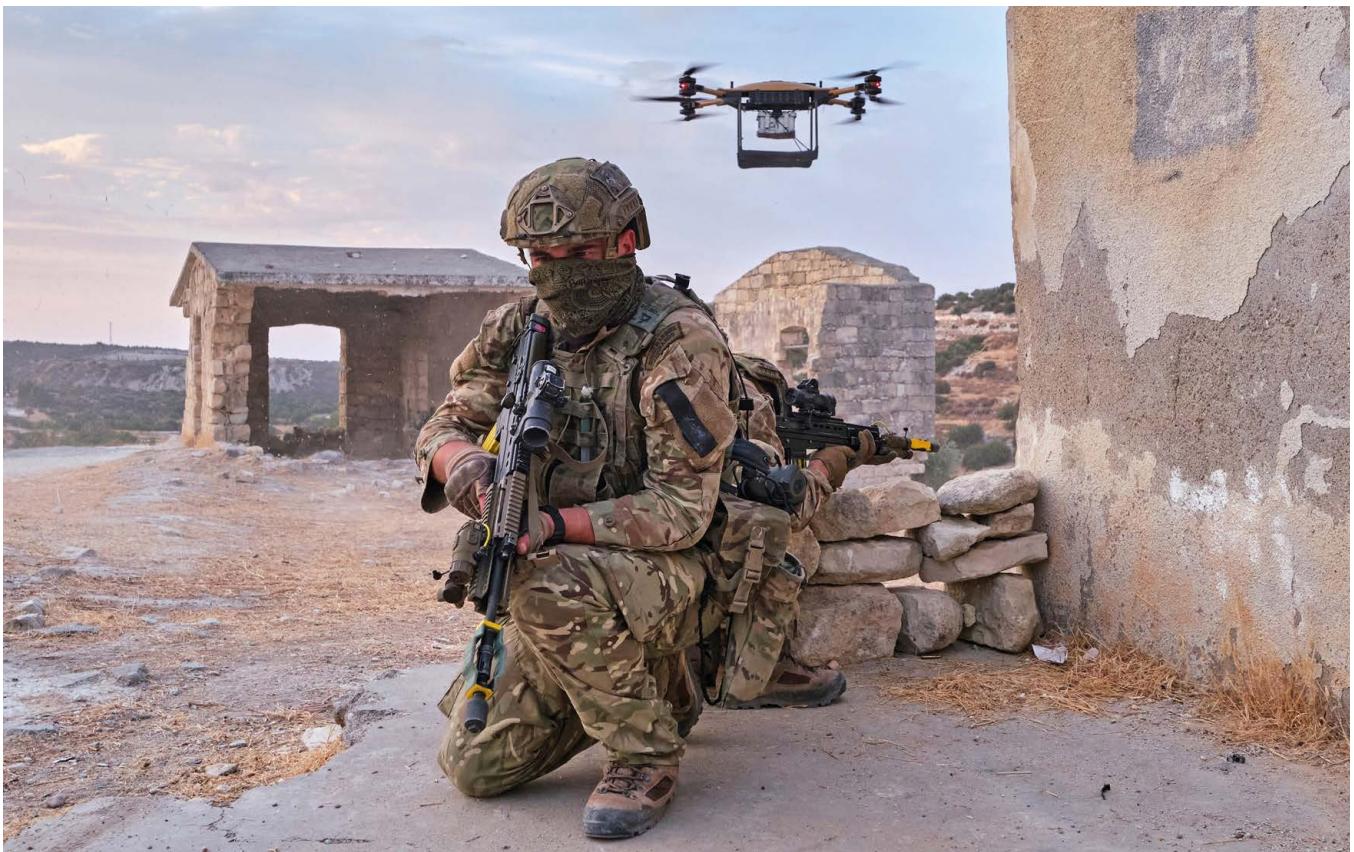
a cutting-edge ecosystem combining people, process, data and technology. Underpinned by enhanced cyber security, technologies will be updated, our workforce digitally transformed, and robust processes implemented to ensure coherence and common standards.

Cloud hosting at multiple classifications is essential to provide the scalable compute needed for our AI models. Cloud-based hosting is already available for Official Sensitive data. **We will deliver clouds at both Secret and Above Secret by end 2022 and 2024, respectively.** Since operational AI use will often rely on sensitive data, we must deliver effective methods of **transferring data between classifications**. Application Programme Interfaces (API) and diodes must also become commonplace to enable us to develop and deploy the latest algorithms at pace and scale.

Advanced sensing, next generation hardware (e.g. ‘beyond CMOS’<sup>20</sup> technologies) and novel ‘edge computing’ approaches will be critical to exploiting AI in Defence, including by creating new opportunities to operate and deliver enhanced capability in challenging, signal denied or degraded environments. **We will therefore invest in R&D and partnerships across Government and with industry to develop and adopt next-generation hardware.**

## 2.2.3 The Defence AI Centre (DAIC)

Alongside the Digital Backbone, we are establishing a **Digital Foundry**, bringing together and building on existing assets to deliver innovative, software-intensive capabilities. This federated ecosystem will be led by Defence Digital in partnership with other Defence exploitation and innovation functions, the S&T community, National Security partners, industry and academia. It is being designed to be the critical next step in the delivery of AI, data analytics, robotics, automation and other cutting-edge capabilities. The **Defence AI Centre (DAIC)** will be a key part



Royal Marine Commandos test a heavy lift drone

of the Foundry – bringing together expertise from Defence Digital, Dstl and Defence Equipment & Support’s Future Capability Group. The DAIC achieved initial operating capability in April 2022 and is now growing to develop the critical mass of expertise to enable us to harness the game-changing power of AI; and accelerate the coherent understanding and development of AI capabilities across the Department. The DAIC will have three main functions:

1. Act as a visionary hub, championing AI development and use across Defence;
2. Enable and coordinate the rapid development, delivery and scaling of AI projects that generate breakthroughs in strategic advantage;
3. Provide access to underpinning pan-Defence digital/data services and sources of expertise as common services to wider Defence.

With the wider Foundry, the DAIC will lead the provision of modern digital and Development, Security and Operations (DevSecOps) environments, common services and tools, and the authoritative data sources that engineers and data scientists require to prototype, test, assure and then deploy their software and algorithms quickly and at scale. AI technologies will be developed across a range of ecosystems (from bespoke in-house solutions to proprietary commercial products) to meet the wide range of potential applications. The DAIC will help guide and cohere technology development, helping establish the appropriate development environment considering the ultimate application of the developed system. It will develop and maintain a **Defence AI Technical Strategy** and **AI Practitioner’s Handbooks** which will guide efforts across Defence, including through appropriate standards and risk assurance frameworks for different defence operating contexts - from military grade AI applications to back office systems - together with underpinning

Testing, Evaluation, Verification and Validation (TEV&V) approaches and technology protection measures. The DAIC will be established with **policy freedoms** to emulate successful ways of working from technology organisations, and will focus initially on optimising existing AI-related work across our S&T, FLC AI exploitation units and Digital businesses.

## 2.2.4 Technical Assurance, Certification and Governance

AI systems present fundamentally different testing and assurance challenges to traditional physical and software capabilities, not least as it can be technically challenging to explain the basis for a system's decisions. This is a significant risk to delivering our strategic objectives. We must strike the right risk balance, ensuring new AI-enabled capabilities are safe, robust, effective and cyber-secure, while also delivering at the pace of relevance – in hours, in the case of some algorithms.

We will ensure that Defence-specific governance aligns closely with national frameworks for AI technologies – encouraging innovation and investment while protecting the public and safeguarding fundamental values. In parallel we will work with global partners to shape norms and promote the responsible development of AI internationally.

**We will pioneer and champion innovative approaches to testing, evaluation, verification and validation (TEV&V), establishing new live**

**and virtual test capabilities**, and collaborating with a broad range of partners. Our S&T programme will work with partners including through the National Digital Twin Programme and the Alan Turing Institute's Data Centric Engineering Programme to develop novel and less risky design, development and testing approaches using digital models and simulations.

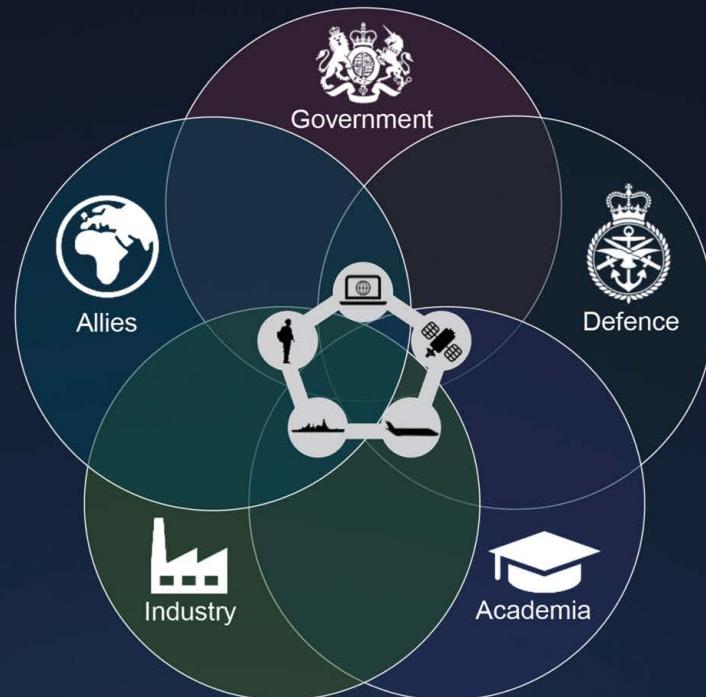
Head Office, the DAIC, **Defence Equipment & Support** and the **Defence Safety Authority** will establish a comprehensive framework for the testing, assurance, certification and regulation of AI-enabled systems – both the human and the technical component of Human Machine Teams. Our approach to AI risk management will be based on the ALARP (As Low as Reasonably Practical) principle that is common-place in Defence for safety-critical and safety-involved systems. **This regime will recognise the importance of appropriate testing through the lifetime of systems, reflecting the possibility that AI systems continue to learn and adapt their behaviour after deployment.**

We will collaborate with other government departments, regulators, bodies such as the Regulatory Horizons Council, Standard Developing Organisations, industry, academia<sup>21</sup> and international partners to drive flexible, evolving yet rigorous **technical standards, policies and regulations** for the design, development, operation and disposal of AI systems – contributing to the Government's aim to build the most trusted and pro-innovation system for AI governance in the world. The OAI will set out a national position on governing and regulating AI in a White Paper due in 2022.

**Trust is a fundamental, cross-cutting enabler of any large-scale use of AI.**

It cannot be assumed – it must be earned. It emerges when our people have the right training, understanding and experience; we have well-regarded ethics, assurance and compliance mechanisms; and we continuously verify, validate and assure AI capabilities within robust data, technical and governance frameworks.

# Multi-Domain Integration Enabled by Artificial Intelligence



Multi-Domain Integration (MDI) is the posturing of military capabilities in concert with other instruments of national power, allies and partners; configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains (maritime, land, air, space and cyberspace) and levels of warfare (strategic, operational and tactical).

Information advantage is critical to achieving MDI. We require the ability to get inside our adversary's decision cycle, and will do so by combining data and information from across all the domains to sense and understand the battlespace. AI will be vital to analyse this information and enable rapid decision-making.

1010  
1010



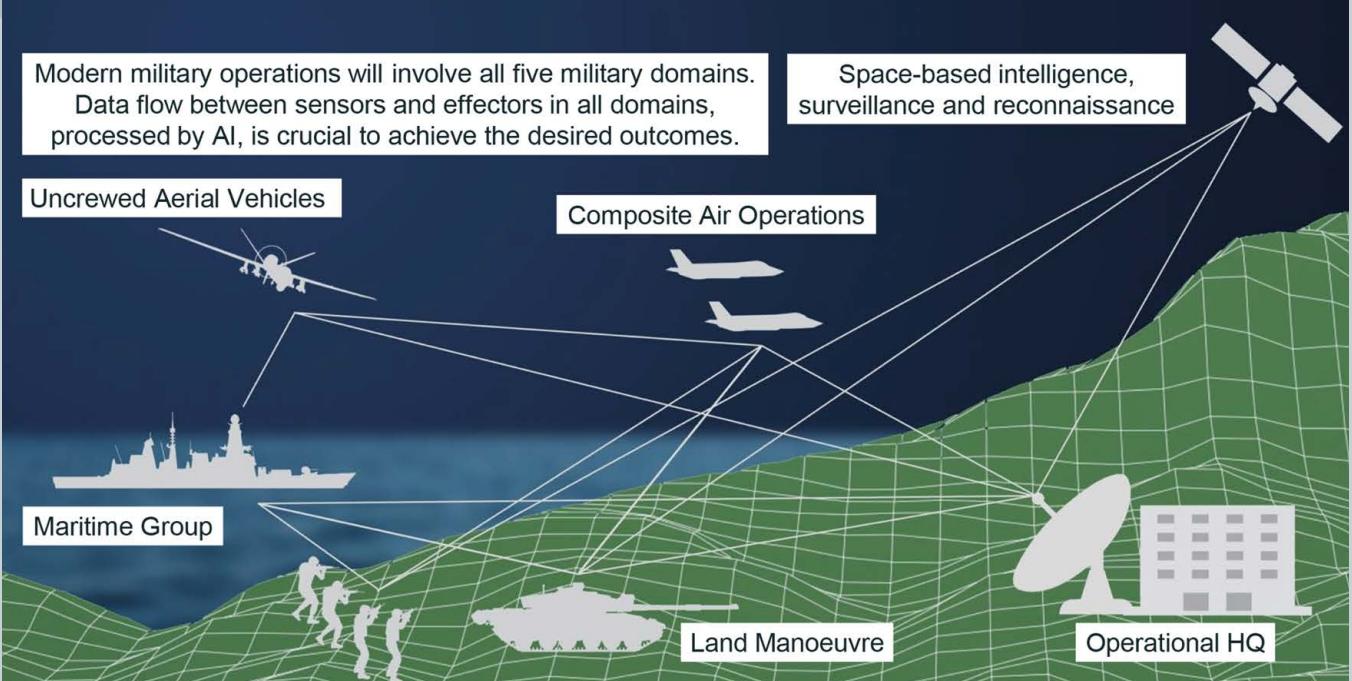
Our battlefields are increasingly data rich. Vast quantities of data are collected from sensors in all domains, including space and cyberspace.

With AI and ML, pertinent and effective data can be utilised and shared in real time, enabling decision making at a pace greater than our adversaries.

Commanders and decision makers, UK defence, allied HQs, and our government partners, require collated and processed data at the speed of relevance.

Modern military operations will involve all five military domains. Data flow between sensors and effectors in all domains, processed by AI, is crucial to achieve the desired outcomes.

Space-based intelligence, surveillance and reconnaissance



# 3. Adopt and Exploit AI at Pace and Scale for Defence Advantage

We aspire to exploit AI comprehensively, accelerating ‘best in class’ AI-enabled capabilities into service; and making all parts of Defence significantly more efficient and effective. To do this, leaders and teams across Defence must excel at the employment and iteration of AI.

The aggregation of gains (big and small) will be a major source of efficiency and cumulative advantage. We must also drive the delivery of ambitious, complex projects which will deliver transformative operational capability and advantage.

The enablers described in [Chapter 2](#) provide the foundation to tackle many of the challenges to rapid and systematic adoption. We will also capitalise on the range of research activities and capability demonstrators already underway, our vibrant national AI R&D base and our strong relationships with allies and partners.

## 3.1 Organising for Success

**AI is not the preserve of a single part of our organisation. Every business unit and Function has an important role to play if we are to achieve our goals.** In line with our delegated model:

- **Head Office** will set overall AI policy and strategy, define capability targets /

headmarks, direct key strategic AI programmes (where appropriate) and ensure the overall programmatic coherence of our AI-enabled capability;

- **Business units and Functional Leaders** across Defence will proactively pursue the forms of AI most relevant to them, guided by this Strategy and direction from Head Office. The majority of delivery will be owned by individual TLBs or capability Equipment Programmes;
- **Strategic Command** will ensure strategic and operational integration of AI-enabled capability across the five warfighting domains. MOD’s Chief Information Officer (CIO) ensures overall digital coherence and delivery of common infrastructure, environments, tools and networks for use across the Department.

Overall strategic coherence of the Department's AI efforts is managed jointly by the **Defence AI and Autonomy Unit** (DAU) and the **Defence AI Centre** (DAIC). The DAU is responsible (on behalf of the MOD's 2nd Permanent Secretary) for defining and overseeing strategic policy frameworks governing the development, adoption and use of AI (e.g. ethical approaches, risk thresholds, cross-cutting issues). The DAIC is the focal point for AI R&D and technical issues: cohering and organising cross-Defence activities; providing centralised services and tools; championing skills and partnerships; and acting as a delivery agent for strategic, joint or cross-cutting AI challenges. An overview of the Defence AI landscape is provided at **Annex A**.

While approaches to capability development, delivery and deployment may need to be reimagined to ensure AI can be exploited at pace, existing Defence 'authorities' (e.g. safety regulation, security accreditation) are broadly unchanged. However, responsible authorities must take account of AI-specific issues and challenges.

## 3.2 Our Approach to Delivery

Our activities can broadly be divided into three categories: (1) **military capability**; (2) **operational and decision support capabilities**; and (3) **enterprise services and the 'back office'**.

Technologically, the key distinction is between '**AI Now**' (mature AI technologies that are available quickly, and which require little or no adaptation for a Defence context) and '**AI Next**' (transformative 'next-generation' and 'generation after next' AI-enabled capabilities).

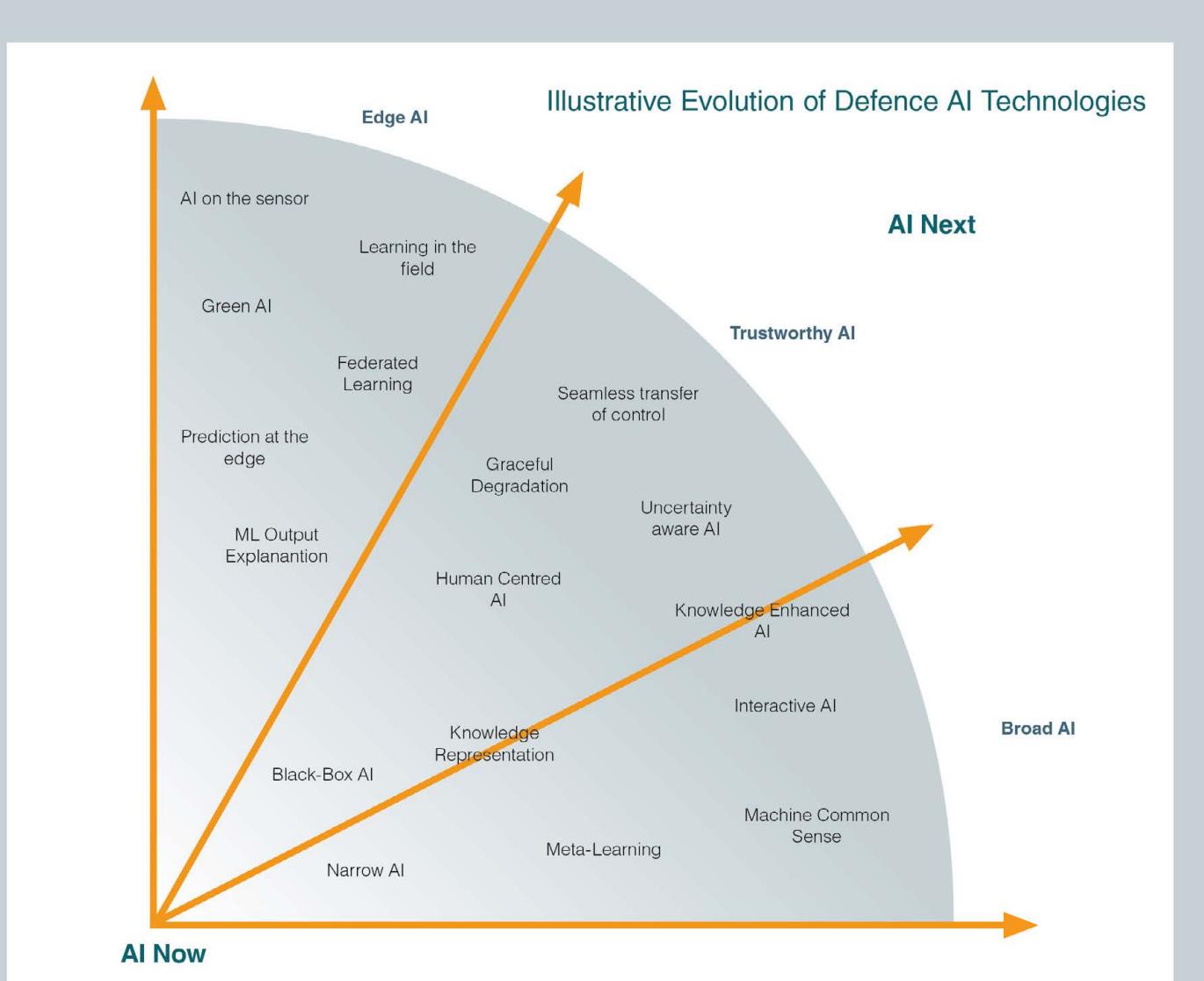
As illustrated on the right, many of the most immediate efficiency and productivity gains for Defence will be delivered through the systematic roll-out and adoption of **AI Now**. Opportunities in this area include the use of mature data science, machine learning and advanced computational statistics techniques to drive smarter financial or personnel management systems, streamlining

## Navigating Technological Complexity

AI encompasses a range of general-purpose enabling technologies. This diagram illustrates the likely evolution of Defence-relevant AI technologies over time, however, in many cases there is significant uncertainty over their utility, transformative effect and timelines to maturity. Technological convergence adds to this complexity, as the combination of AI with other S&T developments (e.g. in quantum, biotech or advanced materials) may unlock game-changing applications or novel military capabilities.

**The Defence AI Centre (DAIC) has a key role helping R&D teams across the department to navigate this complexity**, building an ecosystem to accelerate solutions across the AI "lifecycle" from generation-after-next research and 'AI Next' capability demonstrators (led by Dstl), through to 'AI Now' solutions that can be delivered rapidly into the hands of the User.

The DAIC will promote an agile and innovative environment, learning from best practice across academia and industry, recognising that to succeed it is right that we will invest in some technologies and systems that may ultimately fail or transpire to be 'dead-ends' (e.g. for practical, ethical or security reasons); our approach will be to prototype, test utility and fail-fast if needs be. Incremental development ensures that we iteratively learn what works, the right tools and platforms to use and best practices standards and approaches to adopt. The DAIC will communicate pan-Defence direction and guidance through:



An **AI Practitioner's Handbook**: seeking to capture and disseminate Good Practice from across Defence and industry, providing tailored practical guidance to support:

- Leaders in assessing the full opportunities and implications of using AI solutions;
- AI development teams in understanding the available sources of support and expertise;
- Procurement sponsors in ensuring discussions with suppliers cover the full breadth of requirements and opportunities.

An **AI Concept Playbook**: seeking to spark ideas and constructive engagement with colleagues and partners across academia and industry by setting out the key prospective applications where we see AI having the potential to transform the way we operate or significantly enhance the delivery of military effects.

A **Defence AI Technical Strategy**: Bringing together the technical standards, tools, platforms and assurance requirements that must be applied for Defence AI projects; particularly championing innovation, multi-disciplinary collaboration, open architectures and common systems requirements.

logistics and maintenance, and embracing data fusion and advanced analytics tools to enhance intelligence, surveillance and reconnaissance (ISR) activities. To accelerate AI Now adoption:

- Business units and Functions will identify the portfolio of new projects most appropriate to their needs, reflecting their unique circumstances, challenges and risks;
- We will **publish our strategic headmarks** and develop an **AI Concept Playbook** – a living document which we will update frequently, sparking innovation by setting out the key applications where we see most benefit from AI adoption;
- We will prioritise adoption of **proven techniques from the private sector**, benchmarking our business and support services against comparable organisations, partnering to learn from and emulate ‘best practice’ and exploiting Commercial off the Shelf (COTS) technology - working closely with partners across our own national AI ecosystem. See chapter 4;
- We will delegate responsibility to local teams to identify and acquire or develop the products and solutions needed to achieve desired strategic headmarks – overall programmatic coherence will be managed through the DAIC.

In parallel, we will invest in AI Next: cutting-edge AI R&D designed to tackle current and enduring Defence Capability Challenges where emerging technologies have potential to provide a decisive war-fighting edge. Given the heightened technical and policy risks involved in the delivery of transformational operational capabilities, these activities are likely to be led centrally and, at least in the first instance, driven by the Defence Science and Technology (S&T) programme. Other elements of our R&D delivery system will deliver the capability and capacity to develop, test, integrate and deploy the resulting systems at pace. To accelerate AI Next adoption, we will:

- Maintain horizon-scanning programmes, linked closely to academia and leading players in the sector, to ensure Defence is abreast and keeping pace with cutting-edge breakthroughs in this fast-moving, quickly-evolving area;
- **Prioritise AI as a source of strategic advantage within our Capability Strategies and Force Development processes**, ensuring close collaboration between FLCs, Functional Owners and the R&D community;
- **Commit to ambitious and complex projects**, establishing ambitious capability headmarks to galvanise R&D investment among our partners, accelerate development, and force the pace at which novel AI-driven capabilities and approaches are adopted across the Force;
- Explore the **mandating of equipment programmes to be ‘AI ready’** with an understanding that it may be necessary e.g. for future capital platforms, their sensors and effectors to process at the edge (pattern recognition, command and control, intelligence analysis).

The DAIC will act as our technical coherence authority: determining our requirement for in-house or on-shore assured capability, providing an expert **‘translator’ service** to help leaders understand AI opportunities and implications; and ensuring that lessons and successful approaches are shared widely across Defence (including through the AI Technical Strategy and Practitioner’s Handbooks).

### 3.3 Promoting Pace, Innovation and Experimentation

As we pursue both AI Now and AI Next, we will take a systems approach, recognising (a) that the *integration* of AI into physical or digital systems is perhaps as great a challenge, if not more so, than developing the AI itself; and (b) that we cannot

focus on the technology in isolation, ignoring the other critical elements needed to realise benefits and deliver a genuine new capability. We will:

- **Learn by doing**, tackling comparatively ‘simple’ AI projects – in terms of technical, ethical or operational risk – to deliver rapid evolutionary gains and de-risk more complex activities;
- Embed a culture of **systematic experimentation** to iterate, field minimum viable products, test possibilities, de-risk technologies and training plans, develop new operational concepts and doctrines, and increase our appetite and ability to field AI innovations at pace;
- Deliver AI software through **cross-functional teams**, incorporating end users, technologists (in house, industry and, potentially, academia), capability sponsors and acquirers throughout design and development;
- Ensure AI S&T and acquisition programmes have appropriate procurement, commercial and Intellectual Property strategies for subsequent acquisition and operational activities;
- Adopt new approaches to **agile and rapid capability development and delivery**, applying best practice and lessons from pathfinder projects and Innovation Hubs across Defence, and ensuring that through-life support requirements are considered from the outset;
- Take steps, in accordance with our **Ambitious, Safe, Responsible** approach, to **ensure safety, reliability, responsibility and ethics are central to innovation**.

## Defence R&D is focused around priority Capability Challenges<sup>22</sup>

### Pervasive, full spectrum, multi-domain Intelligence, Surveillance and Reconnaissance (ISR)

- Accelerating technologies with potential to enhance ISR in all domains & environments.

### Multi-domain Command & Control, Communications and Computers (C4)

- Enabling secure, resilient, integrated and coordinated operations and effects across domains.

### Secure and sustain advantage in the sub-threshold

- Competing below the threshold of armed conflict, primarily in the information environment.

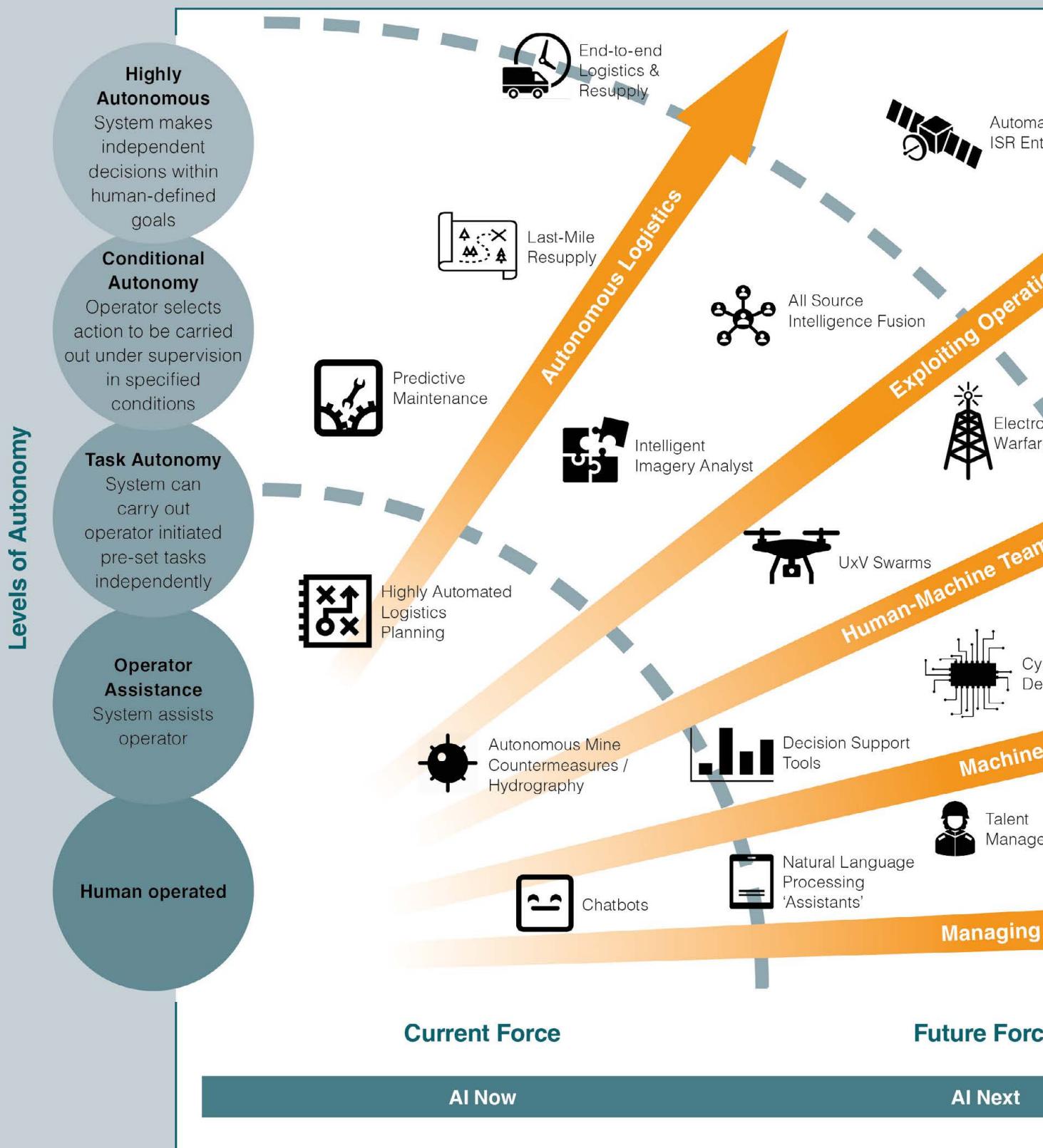
### Asymmetric hard power

- Exploit and counter novel weapons systems (hypersonics, directed energy, swarms etc).

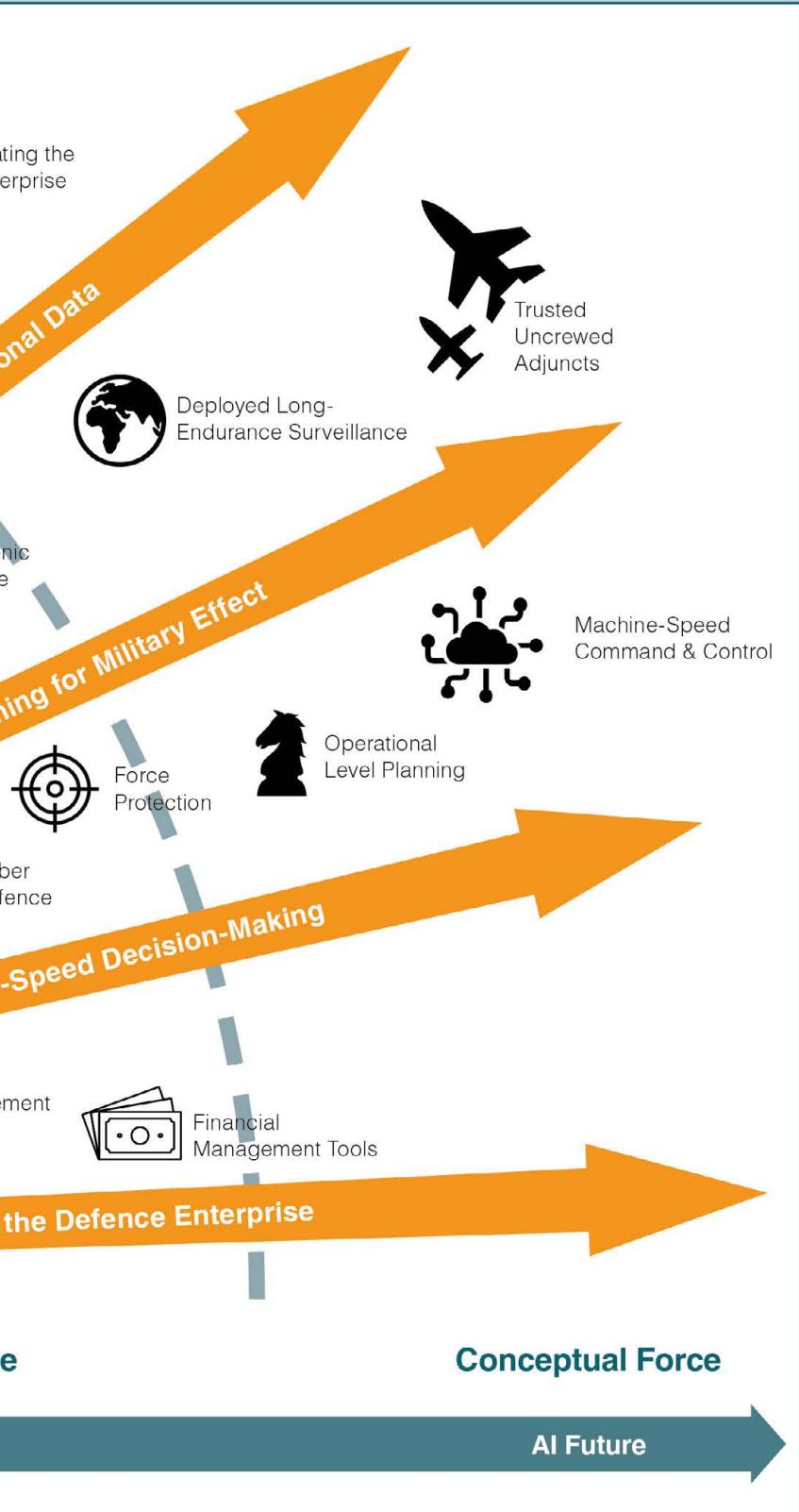
### Freedom of Access and Manoeuvre

- Countering systems that limit our ability to manoeuvre in both traditional and new domains.

# Illustrative AI Opportunities for Defence: Fit for Now and for a Future Force



# in Uncertain Future



## Priority Outcomes

### Decision Advantage



Increase operational tempo and agility through better-informed and distributed decision-making and machine-speed responses to threats.

### Efficiency



Improve flexibility, productivity and availability through intelligent automation.

### Unlock New Capabilities



Secure operational advantage by developing novel ways to operate, deliver enhanced military effect and protect our people from harm.

### Empower the Whole Force



Reduce burdens and focus human talents on higher value functions requiring ingenuity, contextual thinking and judgement.



**Warfighting Experiment 2020 (AWE20):** a Mission Master Uncrewed Ground Vehicle (in foreground) seen here with a recce motorcycle rider as part of a future capabilities demonstration.

### 3.3.1 Securing Our AI Operational Advantage

In increasingly complex and contested security environments, we will need to respond to threats at machine (rather than human) speed effectively and without compromising our values. Adversaries will seek to compromise our AI systems, impair their performance and undermine user and public confidence, using a plethora of digital and physical means. They will also use AI to attack and undermine non-AI systems. Our ability to use AI – while outperforming or otherwise denying the benefits of adversary AI – will be critical.

We must **assess and mitigate AI system vulnerabilities and threats** to both our capability and the data that drives it. We must harden

AI systems against cyber-attack and other manipulations, addressing data, digital and IT vulnerabilities while developing and **continuously evolving security methodologies** for AI capability defence. We must identify and guard against broader AI-enabled threats to capability and operational effectiveness – for example, deception techniques. We must understand the potential cross-domain effects and implications of ‘algorithmic warfare’; develop appropriate counter-AI techniques; and develop appropriate doctrine, policy positions and integrated process to govern their deployment. We must share experience and best practice routinely and at pace, develop effective mitigations and reversionary modes, and integrate these considerations as part of routine command and control

We will establish a ‘joint warfare centre’ to tackle these various AI-related operational challenges,

initially as a virtual federated ecosystem based on the DAIC and Joint Force Cyber Group with contributions from S&T, intelligence, Joint Force Development and our other Warfare Centres (Navy, Land, Air and Space), allied with the National Cyber Security Centre and the National Cyber Force.

## 3.4 Working Across Government

AI will transform the UK's economic landscape, requiring a whole-of-society, all-of-government effort that will span the next decade. The Government has set out its ambition and plans for AI in the **National AI Strategy**. Defence has a critical role to play in preparing and pioneering the use of AI to support both national security and economic prosperity. Likewise, we have lots to gain from working with other government departments to ensure the UK best builds on our strengths in AI.

Defence engagement with partners across government includes:

- Actively supporting the Prime Minister's new **National Science and Technology Council** (NSTC), ensuring a coherent national approach to AI (and other technologies) through the emergent **S&T Advantage agenda**;
- Closely collaborating with related cross-government initiatives to drive cohesion and exploit synergies across the UK's strong AI ecosystem, including with the new **Advanced Research and Invention Agency** and the **UKRI National AI Research and Innovation Programme**;
- Linking with the **Office for Artificial Intelligence** and **AI Council**, seeking to maximise potential prosperity gains from Defence investment in AI and identify opportunities where Defence investments can help to remove blockers to both civilian and military utilisation.

In the national security space, we will:

- Identify opportunities to burden share and collaborate with the Intelligence Agencies and relevant Departments to develop and exploit new AI technologies, including by identifying **common national security AI capability priorities** and establishing a new **Defence and National Security AI Network** to jointly engage with the national AI ecosystem;
- Deepen existing collaborations on AI, such as with the **National Security Technology and Innovation Exchange** (NSTIx), a data science & AI co-creation space that brings together National Security stakeholders, industry and academic partners to iteratively build better national security capabilities;
- Support cross-departmental initiatives to strengthen UK technology protection practices and shape wider global regulatory and counter-proliferation regimes.

## 3.5 International Capability Collaboration

The fastest route to mastering these technologies is to work closely with allies and partners. Our approach to AI will therefore be 'International by Design': sharing information and best practice; promoting talent exchange; developing innovative **capability solutions** to address common challenges; and **sharing the burdens** of maintaining niche yet essential AI development and test capabilities. We will prioritise laying the **foundations for interoperability**: ensuring our AI systems can work together as required (e.g. exchanging sensor feeds and data), that processes are complementary and robust (e.g. for TEV&V), and building trust in the AI-enabled capabilities fielded in coalition operations.



## Mine Hunter – Autonomy in the Royal Navy

The Royal Navy's world-class autonomous mine hunting program can dispose of sea mines while reducing the risk to life of personnel. The system is made up of three vessels capable of working manually, remotely, or autonomously to detect and classify mines and maritime ordnance. Each of the Autonomous Surface Vessels can also tow a variety of equipment configurations to generate combinations of magnetic, acoustic and electric signatures which mimic passing ships to neutralise sea mines. Known as Project Wilton, they are now undergoing comprehensive trials and a capability development program to ensure they are ready to deliver survey operations.

The last vessel to be added to the project, RNMB Hebe, is the largest and most technologically advanced. Hebe has an organic command, control and communications capability allowing autonomous control of her sister vessels. The command centre is fully portable, so mine countermeasure experts can co-ordinate and control the boats or monitor autonomous offboard sensors from onboard Hebe or from a land-based remote-control centre, allowing mines to be neutralised from a remote distance on operations worldwide.

AI software allows a single controller to set the high-level mission objective for the three vessels. The vessels combine to re-optimise the plan during mission, collecting real-time information on new threats and performance, communicating with each other and re-tasking any devices which are free. The systems are being delivered under a £25 million agreement with industry. Project Wilton is operating at the forefront of technological development and paving the way for follow-on autonomous mine countermeasures capabilities currently in development.



© Atlas Elektronik UK

### 3.5.1 Key AI Partnerships

The **United States** is the world's leading AI nation and our most important international partner. The US Defense Budget Request for FY2021 (which allocates \$800m to AI and \$1.7bn to autonomy) demonstrates significant AI ambition<sup>23</sup>. The US has also led the world in championing responsible use of AI in line with our shared values. It is our top priority for AI R&D and capability collaboration, building on our close and long-standing relationship on other technologies and capabilities. The development of our own Defence AI Centre will create fresh opportunities for close collaboration with the **Chief Digital and AI Office (CDAO)**, and we will explore opportunities for enhanced 'service to service' collaboration on shared capability challenges where AI promises game-changing advantage.

We will similarly expand our collaborative efforts through our longstanding bilateral and Five Eyes partnerships with **Australia**, **Canada** and **New Zealand**. Built upon intelligence, data sharing, digital technologies and shared values, these are the ideal frameworks in which to develop AI interoperability. We will also deepen cooperation on AI through the trilateral **AUKUS** security partnership.

**NATO** is our most important strategic alliance and will be a pivotal forum for the UK and Allied consultation on AI and other emerging technologies. **The NATO AI Strategy**<sup>24</sup> (2021) sets out how the Alliance will collectively approach key AI issues, champion the adoption of common standards and principles and promote interoperability. This includes through talent development and fellowship programmes and establishing a network of 'AI Test Centres' – collaborative facilities where NATO institutions and nations can work together to co-develop and co-test relevant AI applications alongside private sector and academic partners.

We will work closely with a range of additional partners, especially in **Europe** and the **Indo-Pacific**, where there is the potential for mutual benefit, and our goals and values are aligned. Many of our close European allies are investing in AI, including through collaborative EU programmes; we will prioritise collaboration with **Germany** and **France**, both of which have announced ambitious plans in 2018 to transform into global AI leaders (the former announced a €3bn seven-year plan; the latter a €1.5bn plan alongside their 'AI for Humanity' strategy). In the Indo-Pacific we will particularly explore options to enhance AI co-operation with **Japan**, **India** and **Singapore**.



Blue Bear Ghost UAS

# 4. Strengthen the UK's Defence and Security AI Ecosystem

The global digital economy has transformed in recent years. Private sector tech investment far exceeds that of governments. Technology titans have become geopolitical powers. Most new and emerging technologies like AI are inherently dual use, and innovation is found across a broad ecosystem of university spin-outs and fast moving small-to-medium scale tech enterprises.

## 4.1 The UK's AI Strengths

The UK is a global superpower in AI and is well placed to lead the world over the next decade as a genuine research and innovation powerhouse, a hive of global talent and a progressive regulatory and business environment. The **National AI Strategy** sets out how the UK will secure its position as an AI Power into the future. The UK has world-class AI and digital industries, with particular strengths in fintech, biotech, digital marketing and advertising and security. Strong tech clusters have emerged nationwide, including in the 'Golden Triangle' (Oxford, Cambridge, London), Cardiff, Belfast, Edinburgh and Manchester.

UK research universities ranked third in the world for most highly cited AI research publications<sup>25</sup>. The UK's higher education system nurtures a diverse skills-base, attracts elite global talent and spins out countless innovative start-ups, complemented by a network of centres of excellence, innovation catapults and business

accelerators, including the Alan Turing Institute, the Digital Catapult, Hartree Centre, Centres of Doctoral Training and Digital Research Infrastructures. Expertise on issues like AI ethics and safety is provided by organisations like Cambridge University's Centre for the Study of Existential Risk and Leverhulme Centre for the Future of Intelligence, and Oxford University's Centre for the Governance of AI and Centre for Long-Term Resilience.

The UK's position as a global AI leader is strengthened by our respected legal system, well-developed regulatory approaches and influential government bodies including the Office for Artificial Intelligence, the Centre for Data Ethics and Innovation, the independent AI Council and the Regulatory Horizons Council. Defence must harness all these strengths to achieve the ambitions set out in this Strategy; collaborating with non-traditional sectors to access elite talent and capitalising on research and dual use solutions developed across the national technology base.

## 4.1.1 Defence's Role in Spurring Technological Innovation

The National AI Strategy set out the government's aim to diffuse AI across the whole economy to drive maximum growth and productivity, including by leveraging the capacity across the public sector to stimulate demand for AI and markets for new services. The public sector will lead from the front, acting as an exemplar for the safe, ethical and rapid deployment of AI.

### Defence and Security Industrial Strategy

The DSIS, on the back of significant increases in MOD's funding through the Integrated Review, is MOD's vision for increasingly closer working between Government, industry, and academia, with greater transparency driving research, promoting innovation, and encouraging joint investment to develop and sustain the industrial capability Defence needs, including through export and international collaboration opportunities. This will bring new and emerging capabilities more rapidly into service, creating military advantage and economic opportunity.

Defence already plays a significant role supporting and catalysing the national S&T and Innovation ecosystem. We steward critical S&T capabilities and invest 50% of our **S&T research budget** with industry and academia. Defence funding and expertise helps shape **national policy, investments, skills programmes and centres of excellence**, such as the UK Cyber and Quantum programmes, the Alan Turing Institute and the Trustworthy Autonomous Systems Hub. Through **Defence Innovation** and initiatives like the **National Security Strategic Investment**

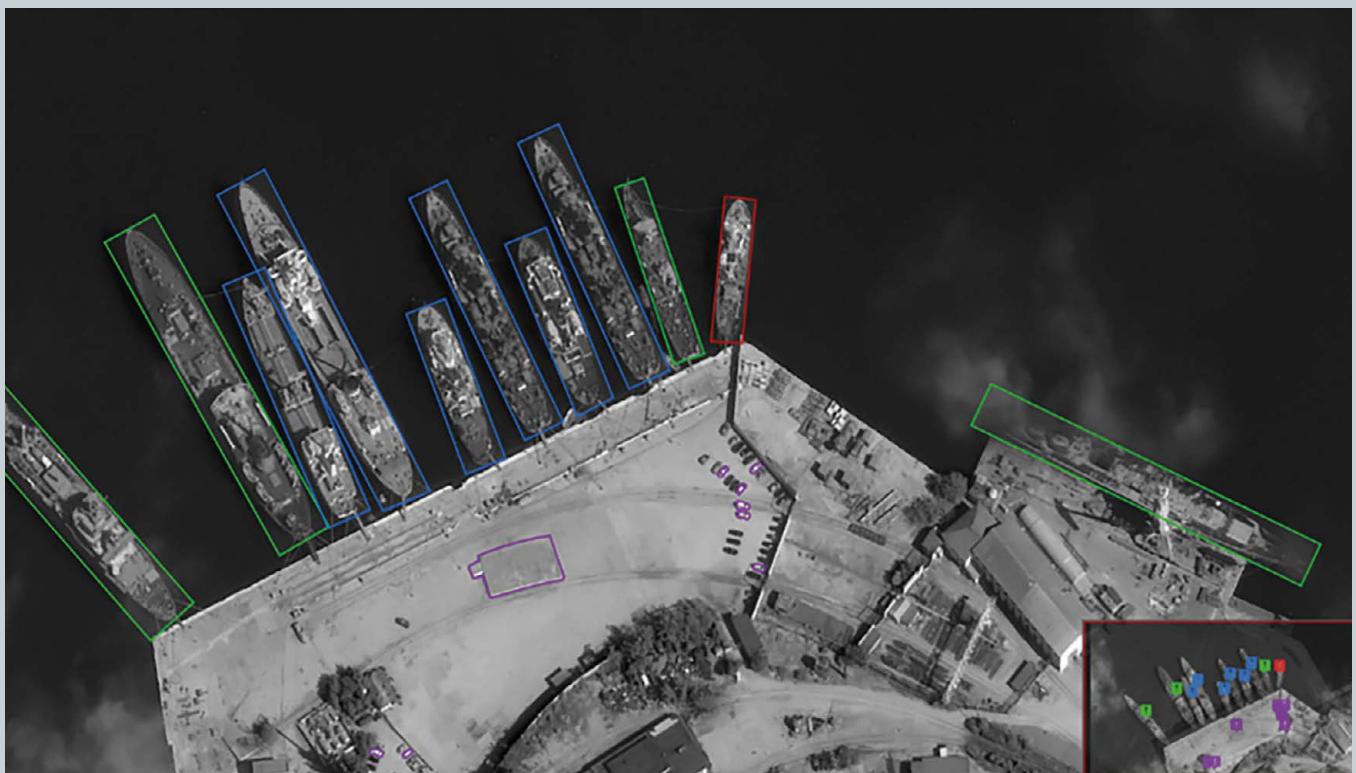
**Fund**<sup>26</sup> we help mature dual-use emerging technologies while 'crowding in' equity investment to shape markets. Our purchasing power stimulates the economy and we often act as a first adopter, de-risking prototype technologies ahead of commercial exploitation. However, we also know that there are a range of **structural and procedural obstacles** that can inhibit new suppliers (particularly small-and-medium sized companies) from working with us.

We have recently launched several **initiatives to streamline processes and tackle key structural blockers**. The **Defence and Security Industrial Strategy**, the **Defence S&T Strategy**, the **Digital Strategy for Defence**, the **Defence Data Strategy** and the **Defence SME Action Plan**<sup>27</sup> all set out how we will address barriers to engagement, provide stronger support to partners and make it much easier to work with us overall. **This Strategy builds on these commitments.**

## 4.2 Partnership on the Basis of Trust

Given the importance of AI to national standing, the UK's AI ecosystem should be recognised as a **strategic national resource** – as vital now as coal and steel were in the industrial age. Defence must play its part in developing and championing this asset. Defence should also be a **natural partner for the UK AI sector**. Collaborating with us offers the opportunity to make a real impact, helping to protect our nation while working on some of the most interesting and challenging real-world technical problems that will shape our collective futures.

Academics and private sector partners demand confidence **that they are working with a responsible actor**. We know this must be a partnership based on trust and that we must earn that trust. We are determined to lead by example. Our approach to the safe and responsible use of AI in Defence will be applied to all AI-enabled



## Image Analysis for Defence Intelligence

Project SPOTTER uses Machine Learning techniques to support and enhance imagery analysts' output, using automated detection and identification of objects within classified satellite imagery. The Centre for Intelligence Innovation has purpose-built graphics processing unit computing capabilities and, using Convolution Neural Network algorithms, has trained the application to identify specific objects of interest. This allows locations to be automatically monitored 24/7 for changes in activity, affording workload prioritisation to improve both the efficiency and timeliness of image intelligence reporting.

The Centre for Intelligence Innovation explored the utility of multiple open-source algorithm frameworks including YOLO, Mask R-CNN and CenterNet to develop models that perform on a range of object types across various biomes. To leverage the maximum benefit to Defence Intelligence, a bespoke application architecture and interface was created; it is scalable, modular and tailored to the analyst's unique requirements.

Project SQUINTER is similar in nature to SPOTTER but is focused on Synthetic Aperture Radar satellite data instead of Electro-Optical. Machine Learning and Computer Vision techniques are being used to detect and identify objects of interest in an automated workflow. The SPOTTER application will be used to host and harness models, presenting analysts with a common user-interface.

The Centre for Intelligence Innovation has accumulated a deep pool of corporate knowledge on how AI and Machine Learning can be specifically applied to support Defence Intelligence requirements. Future work will look to expand the range of objects detected, improve algorithm performance and increase utility amongst various analytical teams. This showcases how AI can be a disruptive technology, by offering analytical insights not currently possible within current limited human resource constraints.

systems and capabilities that are developed and deployed across our business. In addition, we will:

- Be transparent about the ways in which we are using AI, encouraging scrutiny and challenge through our **AI Ethics Advisory Panel** and other fora to provide assurance that AI will only be used responsibly in line with the highest ethical and moral standards and in compliance with our international legal responsibilities;
- Clearly specify through Early Market Engagement how and why we will utilise the algorithms and applications to be developed by our partners, and ensure that pathways exist for individual developers to raise concerns and ask for more contextual information;
- Publish as much information as possible about key safeguards – such as our approach to tackling TEV&V challenges – providing assurance that we will exploit AI systems safely and securely.

To **forge a more dynamic and integrated partnership** with the UK AI ecosystem, ensuring it is geared and incentivised to support Defence requirements and priority national objectives, we will:

- **Clearly communicate our AI requirements, intent and expectations;**
- **Address barriers to frictionless collaboration;**
- **Incentivise engagement and co-creation.**

## 4.3 Clearly Communicating our AI Requirements, Intent and Expectations

We will build confidence and trust by clearly explaining our intent, requirements, and expectations. We already signal our R&D interests

through publications like the Defence Technology Framework<sup>28</sup> (2019), Areas of Research Interest (annual) and the MOD S&T Strategy. We issue regular themed Innovation Calls through the Defence and Security Accelerator (DASA) and engage directly with partners in industry and academia through channels like the Defence Suppliers Forum-Research, Technology and Innovation Group (DSF-RTIG). We will build on these established pathways, working with government partners and, where appropriate, international partners to communicate a scaled demand signal to encourage civil sector investment in defence-relevant AI R&D.

In parallel, it is important to be clear about the unique context and challenges of developing AI solutions for Defence and our expectations for responsible innovation. For example, Defence operational requirements may necessitate a lower tolerance for risk (e.g. acceptable failure rates) than in commercial settings, development and test environments may need to be more constrained, and TEV&V processes may need to consider the potential for accidents, bias, misuse, or adversarial interference. Non-traditional partners will need to be upskilled to understand the implications for their projects and helped to embed appropriate processes, mindsets and security cultures.

We will:

- Work with a broad range of stakeholders (including the Office for AI and the AI Council) to establish a new Defence & National Security AI Network as a forum to share requirements and develop best practice with industry and academia across the range of issues, from policy and technical challenges through to commercial and procurement issues. This will be a key forum to stimulate closer working on Defence-relevant issues and applications, and to identify and advise on regulatory challenges and other opportunities to support the growth of the UK's AI ecosystem;
- Identify where Defence problems overlap with challenges faced by other sectors of the

- economy and work with these non-traditional partners to develop common solutions. This includes dual-use ‘enabling’ industries (e.g. robotics, autonomous platforms, mobile/edge computing) where advances may facilitate the application of AI to Defence challenges, helping us move AI from ‘back office’ data centres and simulation to the real-world front-line;
- Work with the NSSIF to help shape the dual-use ecosystem, access AI capabilities of interest to Defence and, where appropriate, take equity in companies to accelerate

development and capability delivery, while benefiting from subsequent commercial applications;

- Explore opportunities to adapt our commercial and procurement processes to help AI suppliers (particularly those who have not worked with us before) to understand Defence-specific constraints and conditions, and work with academic and industry forums to develop codes of conduct that incentivise a culture of responsible innovation, in line with the following principles.

## Responsible AI suppliers to MOD will be expected to:

- Understand that many MOD capabilities are required to function in contested environments, where an understanding of information security and operational security is critical;
- Focus on solving the key capability challenges faced by MOD, rather than in exploring potential applications of cutting-edge technologies for their own sake;
- Recognise that AI is not the solution to all problems, and that where it is appropriate it will require an understanding of the context of use as well as training for operators;
- Prioritise engaging with the people who will be using and be impacted by an AI system;
- Proactively seek clarification about ethical and safety considerations, understand how these impact technical decisions, and provide proof that products and services meet standards delineated by the MOD;
- Actively pursue and engage with cutting-edge research on technical AI safety, TEV&V, formal methods for verification, and interpretability;
- Take extremely seriously any limitations or potential misuses of the systems they develop. Disclose those limitations to MOD, as well as their uncertainties about systems they develop, in a forthcoming and thorough manner that allows future system owners and operators to diagnose and ameliorate issues with the product;
- Support an open channel of communication with system developers to repair, improve, and test the system. Maintain accountability for the system’s proper functioning throughout its entire lifecycle, including when subjected to periodic stress testing;
- Prove through rigorous testing that the system functions effectively in concert with systems developed by other suppliers. Suppliers should work together from the early design phase and demonstrate interoperability before system deployment, entering a period of troubleshooting to resolve any unforeseen issues.

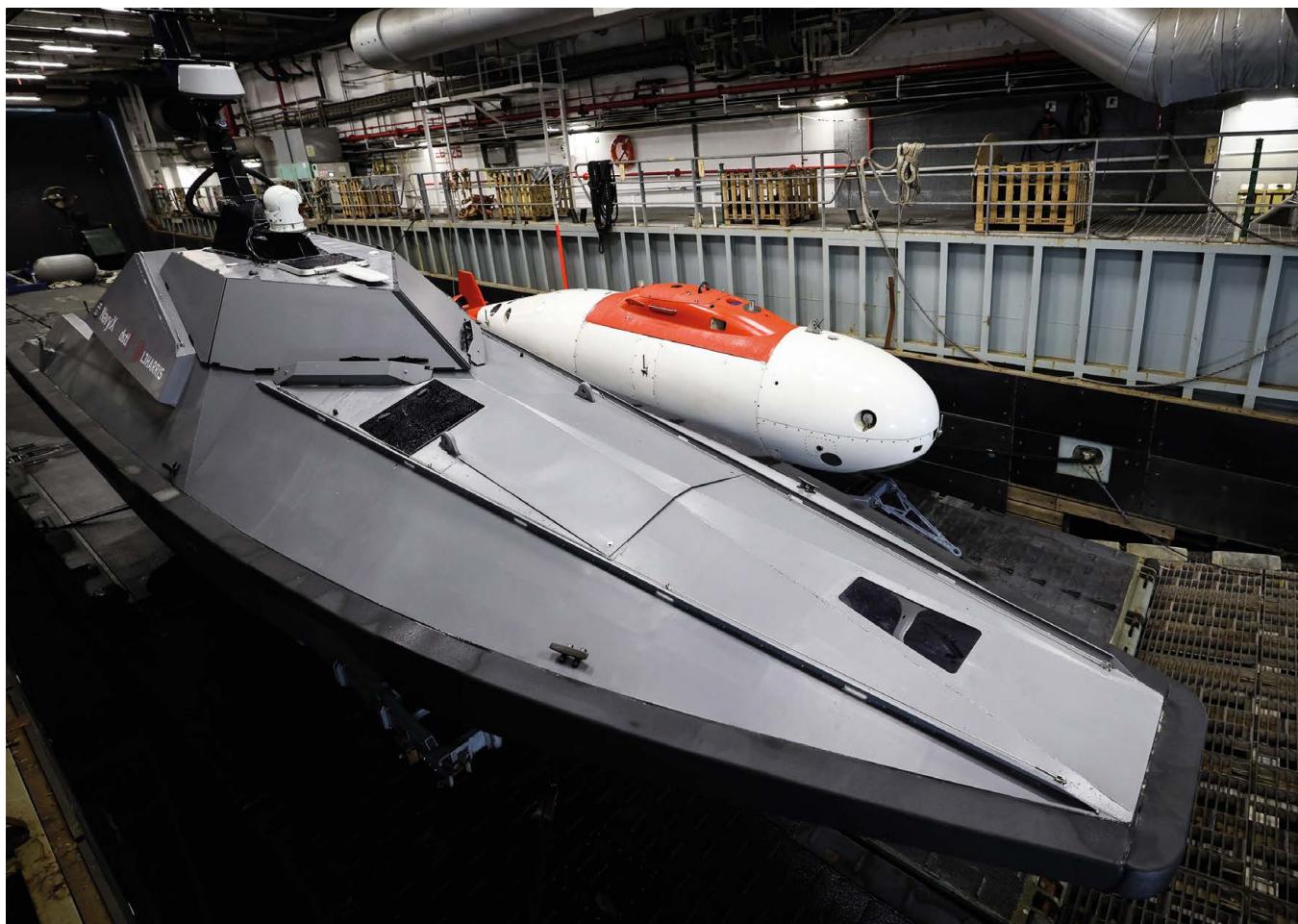
## 4.4 Addressing Barriers to Frictionless Collaboration

As outlined above, we will continue to deliver on commitments in the **Defence and Security Industrial Strategy** and other strategies to address structural barriers and unlock deeper partnerships with all aspects of our AI ecosystem, at all levels of technology maturity and across the technology stack. These commitments include increasing transparency on our longer-term priorities, engaging with industry early on potential solutions to capability requirements, reducing barriers to Small and Medium Enterprises and more joint working to provide firms with the confidence to invest in developing

new technologies. We will also work with cross government partners, suppliers and international partners to ensure appropriate protection for critical AI capabilities and Intellectual Property (set out in [Chapter 5](#)).

### 4.4.1 Information Age Acquisition and Procurement Policy

As part of continuing **improvement of the acquisition system**, we are testing more rapid processes for acquiring cutting-edge technology which will enable Agile methodologies to be embedded across the end-to-end acquisition



*Madfox Autonomous Surface Vessel alongside an Extra Large Uncrewed Underwater Vehicle (XLUUV) built by MSubs in Plymouth.*

system. In addition, we are streamlining commercial models for AI and digital delivery so we can contract at a pace that matches the short turnaround times that are essential for agile and disruptive Tech companies.

We will work through both the new **Defence and National Security AI Network** and the **Defence Suppliers Forum SME Working Group** to understand the challenges facing smaller suppliers, including reducing the barriers that prevent viable companies – particularly SMEs – from entering our supply chains.

We will learn lessons from our Innovation ecosystem and roll out best practice across Defence. For example, we will explore opportunities to streamline procurement for ‘small’ value digital purchases, reflecting the need to smooth the procurement path from proof of Concept through to the purchase of digital products and services.

## 4.5 Incentivising Engagement and Co-creation

Consultations with partners across the UK AI sector have highlighted the following key factors:

### 4.5.1 Understanding and Reflecting Market Forces

Defence must understand – and be seen to understand – the market forces and processes which actually incentivise companies in the AI sector. This understanding must then be reflected in both our approaches and AI-related communications. We will therefore establish **a dedicated Industry Engagement Team** within the Defence AI Centre, staffed by a mixture of Crown Servants and secondees from the private sector, to ensure we are properly attuned to the perspectives

and needs of our industry (and academic) partners and regularly test approaches through the **Defence and National Security AI Network**.

### 4.5.2 Talent Exchange

Chapter 2 of this Strategy sets out measures to uplift AI skills and understanding across Defence. A key role for the new Engagement and Interchange Function within the Defence AI Centre will be to develop closer links with AI training institutes, universities and professional bodies to highlight the opportunities and impact of working in Defence, dispel myths, and catalyse a two-way flow of talent. We will strengthen existing links with UK universities, providing clear information for the benefit of academics interested in working with us on issues like information handling. We will also partner with the AI Council and other stakeholders and forums to communicate a better appreciation of our skills requirements from the AI industry and Tech Sector generally, while holding competitions and hackathons to identify and attract emerging talent.

### 4.5.3 Simplifying Access to Defence Assets

We will **champion open systems architectures** to avoid vendor lock-in and promote optionality, and take steps to **unlock Defence data** in line with Government’s wider approach set out in the **National Data Strategy**. This includes collaborating on the development of the **Information Management Framework**, led by the Centre for the Protection of National Infrastructure (CPNI), covering the technical and non-technical frameworks necessary to enable complex, multi-party, secure data sharing. Data is the lifeblood of AI systems, and developers need access to large volumes of quality, curated data to train and tune their algorithms. Greater access to Defence data is therefore a key element of our new compact with the UK AI Sector. However, while Defence holds unique large-scale datasets, much of this data can

be stove-piped, poorly curated or highly classified, limiting the scope for partners to practice, learn and develop innovative applications.

Wherever possible, our approach will be to require information owners to provide open access to curated datasets to maximise the potential for sharing and experimentation, while working with industry and academia to develop scalable solutions to data labelling challenges. Automated (pseudo) anonymisation techniques and Privacy Enhancing Technologies may enable analysis without revealing underlying details. Where this is not possible or appropriate (for example operational or platform-sensitive data), we will explore options to develop and share **representative, synthetic datasets**, managed by the Defence AI Centre.

We will increase access to **niche Defence capabilities**. Along with training data, the AI development community needs access to compute power and representative digital test environments to safely experiment and refine the functionality of their products. As a core part of our offer, we will provide far greater access to the **specialist computing capabilities and test & assurance infrastructure** that we maintain, learning lessons from similar government initiatives like the FSA's regulatory sandbox pilot for the financial sector<sup>29</sup>. These capabilities are not otherwise available to UK academic and industry partners yet are often essential to push the boundaries of what is possible within extreme Defence operating environments.

#### 4.5.4 Promoting Co-creation

'Co-creation' brings together government users with suppliers to encourage a seamless exchange of ideas and data, iterative prototyping and rapid development at a pace and scale that could not otherwise be achieved. We will increasingly diffuse our world-class technical expertise into specialist regional co-creation spaces across the UK to

enhance engagement and collaboration with the AI sector, drive **prosperity** and support **Levelling Up** and the **Union**. We will:

- Deepen existing regional collaborations on AI, including through: Dstl's new **AI lab in Newcastle**; Command-led innovation centres (such as the Defence BattleLab at Winfrith); **National Security Technology and Innovation Exchange** co-creation hubs; and increasingly close working with other government initiatives such as **NHSx**;
- Continue to exploit DASA's network of regional **Innovation Partners** to help AI innovators in business and academia to understand and access Defence opportunities and assets;
- Make increasing use of the growing network of **Regional Defence and Security Clusters** that MOD is supporting industry and Local Enterprise Partnerships in piloting across the UK, building on our experience from the recently established South West Cluster;
- Explore opportunities for **thematic AI co-creation clusters** around the UK that can leverage multi-disciplinary groups of industry and academic specialists to target key missions from our AI Playbook.

The Defence AI Centre will have a key role in delivering these commitments, acting as the focal point for engagement to ensure that we can access the best cutting-edge expertise, techniques, standards and new ideas from across the national AI and wider technology base.

#### 4.5.5 Business Support Services

Innovative AI start-ups often require a range of business support services to incubate products and navigate access to funding streams<sup>30</sup> necessary to scale up and compete. We will help AI companies access trusted sources of

business development advice, equity finance and investment, through programmes like the **Defence Technology Exploitation Programme** and **Defence Supply Chain Development**; while exploring options to expand the Defence and Security Accelerator's **Access to Mentoring and Finance** service to provide greater support for small-to-medium sized AI companies.

In addition, we will:

- Develop new approaches to maximise the exploitation and commercialisation of Defence-held AI-related intellectual property through **Ploughshare Innovations Ltd**;

- Champion **enhanced global market access** for the UK AI sector so that innovative UK tech companies can secure that growth capital and consumer scale necessary to compete at a global level. On behalf of UK industry, the UK MOD, through its membership of the U.S. National Technology and Industrial Base (NTIB), is working closely with partners in the US Department of Defense, the Department of Defence of Australia, the Department of National Defence of Canada, to strengthen and build resilience in our respective industrial bases, enhance innovation and reduce barriers to the flow of knowledge, goods and services.



Milrem Robotics THeMIS Uncrewed Ground Vehicle

# 5. Shape Global AI Developments to Promote Security, Stability and Democratic Values

As AI becomes increasingly pervasive, it will significantly alter global security dynamics. On the one hand, it provides opportunities for enhancing, implementing, monitoring, and enforcing global governance structures. On the other, economic disruption may cause instability; public disquiet about the impact of algorithms may increase; and military AI use may change the character of conflict.

Some AI-driven issues may be subtle and insidious; whilst AI systems have the potential to enhance democracy and transparent governance, authoritarian regimes are using them to increase surveillance and repression. Manipulative techniques like ‘deep fakes’ may increasingly be used to undermine democratic processes. Other issues may be more dramatic; we must be alert to the possible emergence of destabilising new capabilities (including new weapons of mass destruction or mass effect), attempts to obscure responsibility for illegal or malign use, and accidents or misunderstandings involving AI-enabled systems.

AI will be an important area of geostrategic competition, not only as a means for technological and commercial advantage but also as a battleground for competing ideologies. We need to understand the varied terrain on which these ‘battles’ will be fought – in terms of technology,

data, systems, norms – and marshal the various levers at our disposal to best effect. Amidst this geo-strategic complexity, and working closely with wider Government, allies and partners, our goals within Defence are to:

- **Shape the global development of AI in line with UK goals and values** – promoting responsible approaches and influencing global norms and standards, in line with democratic values;
- **Promote security and stability** – countering harmful technology proliferation and exploring mechanisms to build confidence and minimise risks associated with military AI use;
- **Develop future policy approaches** – investigating strategic AI-related risks and issues, and addressing them proactively with allies and partners.

# SAPIENT: Autonomous Security System that Reduces Operator Workload

Sensing for Asset Protection with Integrated Electronic Networked Technology (SAPIENT) is a network of advanced sensors with AI at the edge, combined with intelligent fusion and sensor management.

Most security systems, such as CCTV cameras, simply collect data and feed it to an operator who assesses the situation and directs the system accordingly. Monitoring and interpreting lots of data can place a high cognitive burden on the operator. In the SAPIENT system, individual sensors make low-level decisions autonomously, such as which direction to look or whether to zoom in, in order to fulfil a higher-level objective. These higher-level objectives are managed by a decision-making module which controls the overall system and makes some of the decisions normally made by the operators. This reduces the need for operators to constantly monitor the output of the sensors.



SAPIENT is a MOD-owned, open-architecture that specifies the standards and protocols that allow modern AI algorithms to work in concert across a suite of sensors. These algorithms reside both on-board the autonomous sensor modules (ASMs) (embodiment AI at the edge) and at decision making modules (DMMs). The architecture strongly encourages component modularity (the ability to plug-and-play these modules) which reduces system integration time and creates a competitive supplier ecosystem for the components.

Critically, SAPIENT is designed to enable multi-sensor fusion (correlation, association and tracking) and sensor management (dynamic tasking of the sensors in response to the unfolding scenario). This gives MOD access to the advanced AI solutions that are being developed by our innovative supplier base. Whilst the key outputs from the SAPIENT initiative are the standards (embodied in the Interface Control Document (ICD), test harnesses and other software tools) to enable innovative suppliers to develop ASM and DMM components, the SAPIENT project has also developed research versions of these components to demonstrate the concept and evaluate the benefits to users.

SAPIENT has been demonstrated in realistic base protection scenarios with live sensors and targets, and in a mock urban battlefield flagging dangers to soldiers. Often this included very little or no software engineering, even being completely plug-and-play with zero-second integration time, delivering great support to command and control of operations in complex terrain.

**Above:** SAPIENT was trialled during the Contested Urban Environment (CUE) 2021 international exercise held in Portsmouth.

## 5.1 Shape the Global Development of AI in Line with UK Goals and Values

AI is transforming the world around us, but its forms, uses and impacts are not pre-determined. Effective intervention and influence can significantly reduce risk and increase benefit for the UK and its allies and partners. It is therefore essential that we maximise our ability to shape global trends in the development and use of the technology, especially where these issues concern our core values. We will be most effective when we collaborate and build coalitions with like-minded nations – but we will look broader than this, also working with those who are traditionally less aligned with the UK in these areas, so we can understand and – where appropriate – incorporate their views and concerns.

### 5.1.1 Promote Safe and Responsible Military Development and Use

We are clear that we seek to maximise our operational capability through the use of AI, but also that there must be no ‘race to the bottom’ – no pursuit of capability without regard for responsibilities and safeguards. The UK has an important role to play in avoiding any such downward spiral and has long been at the forefront of shaping the open international order. International Humanitarian Law provides a robust, principle-based framework for the regulation of weapons development and use, focusing on effects rather than the nature of any particular technology. It imposes positive obligations that take account of core principles – distinction, necessity, humanity and proportionality – and is the most appropriate way of regulating new means and methods of warfare.

AI is a general-purpose technology which contributes to systems, potentially including weapons systems, in different ways and supporting different ends – but nothing about AI fundamentally changes our obligations under UK law and international law, or the importance we attach to the standards, values and norms of the society we serve. **We have set out our own approach and we encourage other nations to do the same;** such public declarations are an important aid to understanding, scrutiny and dialogue.

Our approach will underpin our efforts to forge a global understanding on the responsible uses of military AI, aligned with UK values. **We will work closely with allies and partners to build consensus, promote a common vision for the safe, responsible and ethical use of these technologies globally, and push for compliance with International Humanitarian Law.** The UK is deeply committed to multilateralism, and we will continue to play a leading role within international discussions to strengthen institutions and adapt them to the changing face of technology. It is right that we continue to place importance on the UN Convention on Certain Conventional Weapons (CCW), which discusses ‘Lethal Autonomous Weapons Systems’ (LAWS). The CCW’s discussions will remain central to our efforts to shape international norms and standards, as will our support to wider Government in forums such as the Global Partnership for Artificial Intelligence and the Council of Europe.

Our immediate challenge, working closely with allies and partners, is to ensure ethical issues, related questions of trust, and the associated apparatus of policies, process and doctrine do not impede our legitimate, responsible and ethical development of AI, as well as our efforts at collaboration and interoperability. We strongly welcome the publication of ethical principles by close allies such as the USA and France, and NATO’s leadership of ethical debate within the Alliance. We will continue to engage actively in the US-led **AI Partnership for Defense**, which brings together like-minded nations to advance AI ethics, taxonomy, Trusted AI, and Skills.

We will continue to work with the UN, other states, civil society, industry and academia to develop and promote best practice in the use of AI and autonomy in weapons systems. We will be open to a wide range of measures to do this. These may include: codes of conduct; a series of positive obligations or commitments; or new reporting or verification mechanisms. We will actively share our extensive diplomatic, technical and legal expertise in doing this, but we cannot stop at this – we must ensure that international systems have the ability to enforce norms and standards effectively, holding to account those who do not abide by them.

## 5.1.2 Influence the Global Development of AI Technologies

The **Integrated Review** highlights the likelihood of intense competition over the development of rules, norms and standards governing technology and the digital economy, and the particular importance therefore of active diplomacy to influence these frameworks. We have a key interest in this activity. We recognise the importance of using normative and regulatory frameworks to shape markets, promote stability, and reduce opportunities for adversaries to use technologies to cause us harm. We also need regulations and standards to support and enable our own preferred uses of AI.

We will therefore play a key role supporting UK regulatory diplomacy, contributing our S&T expertise and experience in relevant fields like cyber regulation. We will help to ensure that the UK's approach to AI R&D supports wider strategic goals, following the Integrated Review's 'Own Collaborate Access' approach. We can promote certain values by creating technologies that enable them; as a significant actor in UK R&D and major future user of AI, we can encourage research and development of AI systems which advance the open and democratic use of AI, in particular trustworthy and explainable AI. Working with industry and academia, we will

explore opportunities to **shape the landscape of AI competition** to give our values a structural advantage.

## 5.2 Promote Security and Stability

Like any significant technology or capability, AI has the potential to disrupt the balance of power between states or in particular regions. This challenge is exacerbated by the nature of the technology – increasingly pervasive and, in some senses, easy to acquire. Advanced applications can be found across many industries, with technologies like small drones becoming increasingly accessible. The novelty of some applications creates risks of miscalculation or misunderstanding. 'AI Power' – like 'cyber power' – is much vaunted but difficult to measure and monitor.

### 5.2.1 Counter-proliferation and Arms Control

While recognising that many forms of AI will be ubiquitous and easily accessible, we must nevertheless take steps to limit the spread of key strategic or sensitive technologies or techniques. We must be particularly concerned about the deliberate transfer of technology by states to non-state or proxy actors. **We will work with allies and partners to address the potentially destabilising effect of AI proliferation.** We must reinforce, reinvigorate and adapt, balancing the opportunities of new technologies with appropriate controls to constrain access to 'military grade' AI applications. Where appropriate, we will work through existing non-proliferation, disarmament and export control regimes, treaties and organisations to ensure we balance the opportunities of new technologies with appropriate controls. We will:

- Closely monitor trends in technology, preparing for the risks of dual-use technologies, or the risks that AI will exacerbate existing counter-proliferation and arms control challenges;
- Focus on restricting the movement of components and hardware that significantly enhance capability; and on applying appropriate controls to the movement of data;
- Support cross-Whitehall strategic international engagements on S&T, to ensure a clear-eyed approach on the risks of dual-use technologies such as AI;
- Work with international partners to develop means of preventing AI proliferation or misuse.

AI can itself play a key role in enabling us to achieve these goals. Where appropriate, we

will use it to: help identify risks; make reporting mechanisms more effective; strengthen our enforcement capability; ensure controls are applied effectively; and allow swifter verification of potential concerns.

## 5.2.2 Protecting Critical Technologies

Our AI ecosystem is fuelled by open knowledge, information and data flows, particularly within academic research environments. This openness is a great strength, encouraging a healthy influx of domestic and foreign investment that has helped catapult scientific and technological ideas into world-class products, solutions and services.

However, as the **Integrated Review** has made clear, our openness is increasingly being exploited



**Autonomous Advance Force 4:** Royal Marines carried out experimental exercises with a range of drones to further develop tactics and techniques with autonomous systems.

by adversaries for military and economic gain. Areas of concern are broad, including academic interference, penetration of sensitive research areas, acquisition or control of key strategic technology companies, risks of Intangible Technology Transfer and proliferation, Intellectual Property theft, tampering, and reverse engineering. Adversaries like Russia and Iran are particularly active threats in this respect. Likewise, China's military-civil fusion strategy provides clear strategic direction to further integrate civilian and military research and industrial developments, raising the risk that R&D partnerships or dual-use technology acquisitions may directly benefit their defence industrial base and broader national security apparatus. While Military Civil Fusion has broader purposes than acquiring foreign technology, in practice it means there is not a clear line between Chinese civilian and military economies, raising due diligence costs for nations and global entities that do not desire to contribute to the Chinese military modernization.

Effective technology protection is critical to secure future military edge, safeguard UK intellectual Property, and fulfil our obligations to prevent the proliferation of military and dual-use goods, software and technology. This is a significant challenge given that the threats to our R&D sectors are not yet clearly understood and are evolving rapidly as novel technologies mature. We will:

- Deepen our understanding of the UK's comparative AI strengths and weaknesses (including hardware dependencies), defining critical component technologies where: (a) the UK requires onshore assured access; (b) we should prioritise collaboration with likeminded allies; or (c) the ubiquity of the technology poses minimal security risk;
- Determine whether our unique requirements necessitate more stringent measures for acquiring AI products, services and underlying technologies. While we are committed to strengthening the UK AI ecosystem, and our starting assumption is that most commercial, dual-use 'AI Now' technologies may be

appropriate for global competition, exploitation of – or bespoke technology development for – 'AI Next' is likely to require enhanced protection (potentially including assured onshore access where we need operational independence);

- Selectively intervene to ensure strategically-important UK companies and capabilities are supported and protected from foreign investment, where the national interest demands it;
- Deploy the technology protection levers at our disposal in a measured and targeted manner, including powers under the National Security and Investment Act, checks within the Academic Technology Approval Scheme and provisions within export control regimes.

## 5.2.3 Build Confidence and Minimise Risk

We must nevertheless expect increasing numbers of AI-enabled force elements in real or virtual theatres of operations, and for them to operate at increasing speeds. They may be hard to distinguish from more conventional forces, but display unexpected behaviours. This could be intentional, the unexpected consequences of various system interactions, or the result of cyber-attack or some other manipulation. Some capabilities will simply malfunction, especially if safety and reliability standards are compromised in the rush to field new battlefield capability. Increasing numbers of autonomous platforms and reduced human involvement in (or even control over) operations could alter conflict thresholds and create spirals of violence and escalation.

We must take appropriate steps to limit the possibility of misunderstanding, miscalculation or uncontrolled escalation arising from these factors. At times, it may be crucial to know whether or not a system was AI-enabled or not, and to what degree. This could be particularly important in the event of a crisis or flash-point,



## Automation in Data Analysis

In an environment where data is ubiquitous it is increasingly important that intelligence analysts can automate the collation and analysis of large datasets. The KILPECK programme is working to enable this through establishing an operational data science environment, where datasets from Official through to Top Secret are stored and accessed by the analyst. Using an Activity Based Intelligence methodology, all data is georeferenced to enable the rapid integration, exploitation, and production of intelligence. Analysts can write their own code or use coded notebooks (with 25 in development), which have been written by the data science community to rapidly exploit these growing datasets. Enabled by a full audit and compliance regime, any code executed by analysts is accompanied by a 'model card' which explains what the code is doing, and how it is transforming the data. By automating much of the collation process, intelligence analysts are pushed up the value chain and can focus on contextualising the data and providing assessment.



or in the already murky context of sub-threshold activity. **We will engage with allies and partners to understand these issues and develop proposals for codes of conduct and other confidence-building measures which can reduce the risk of accidental engagements, collateral damage, and miscalculations.** We will also share best practice internationally on how to conduct TEV&V and weapons reviews, such as practical descriptions and case studies regarding the use and parameters of system control, where appropriate. **In this context, it is critical that we engage with potential adversaries and nations whose approach to adopting AI differs from our own, and that we strongly advocate safe and responsible use.**

## 5.3 Develop Future Security Policy

AI technologies are evolving rapidly, and associated security risks and issues with them. We must maintain a broad perspective on implications and threats, considering extreme and even existential risks which may arise, and ensuring our risk management practices acknowledge and are suitably adapted to the uncertainty. We must ensure that our technological understanding of AI futures, developments and trends (including investment markets) – derived mainly through our S&T programme and engagement with the wider expert community – informs our broader analysis, strategy and posture. Innovative and disruptive applications (which are inherently hard to predict) have already had a significant impact on numerous industries and business models. The challenge for security policymakers is to understand – and even to anticipate – and address key AI-related strategic changes.

We must understand how AI trends intersect with other factors – economic, demographic, political, societal, diplomatic, the strategic power of ‘Big Tech’ – and how AI may drive important dynamics, incubate novel threats, or otherwise undermine global security. The automated

production of disinformation and use of ‘deepfakes’ could exacerbate ‘lawfare’ against our forces, dramatically undermine public support for UK operations or even, in extreme circumstances, overwhelm and paralyse critical national decision-making. Increasing global technology fragmentation or resource chokepoints (e.g. linked to semiconductor supply) may become increasingly strategically significant.

We will support the **National Science & Technology Council** and the **Office for Science & Technology Strategy** to develop broad perspectives on these strategic implications, providing unique Defence expertise, intelligence, analysis and insight – e.g. through wargaming, red-teaming and scenario-based investigations. We will engage closely with allies, partners, academia and civil society to drive forward strategic studies and build the capacity to understand and anticipate the strategic impacts and risks of AI in defence. Recognising AI’s profound impact across many sectors, we will seek to learn lessons from areas (e.g. Finance) which have devised protocols to limit shocks despite highly competitive and fast-paced environments.

### 5.3.1 AI, Strategic Systems and Deterrence

There is a potential risk that strategic stability could be undermined by the development of new weapons of mass destruction or mass effect, or by the integration of AI within strategic systems. Nuclear deterrence postures and calculations are already complicated by the emergence of new threats to space-based communications and early warning systems, and by the broader, more amorphous cyber threat to digital systems. With its myriad possible applications, AI has the potential to disrupt strategic paradigms further, for example by encouraging machine-speed escalation. Conversely, AI could have the ability to improve strategic stability, for example by allowing more complex modelling, better-informed

decision-making, and therefore reduced risk of miscalculation and unintended escalation.

The UK is at the forefront of work internationally to reduce the risk of nuclear conflict and enhance mutual trust and security. We will champion strategic risk reduction and seek to create dialogue among states possessing nuclear weapons, and between states possessing nuclear weapons and non-nuclear weapon states, to increase understanding and reduce the risk of error, misinterpretation and miscalculation. We will study the effects of AI on the inter-linked domains of cyber, space and nuclear, examining AI's potential to accelerate or amplify developments linked to other emerging and strategic technologies. We will promote and engage with international dialogue aimed at identifying and addressing crucial AI-related strategic risks. **We will ensure that – regardless of any use of AI in our strategic systems – human political control of our nuclear weapons is maintained at all times.** We strongly encourage other nuclear states to make a similar commitment.

As an enabling technology, AI is not itself a threat, and we will seek to use AI, where appropriate, to help tackle and reduce the threats we face. We are aware however, that adversaries are likely to seek to exploit AI to increase the harm they can do to us. A robust position on deterrence is at the heart of the Integrated Review. **We will maintain the effectiveness of our deterrence strategies and capabilities in the face of new threats, opportunities or other changes to the security environment driven by AI.** We will devise new strategies as required to address specific AI-linked threats, while continuing to champion positive and responsible uses of AI. If threatened or attacked by an AI-enabled adversary, we will consider not just the harm caused but also the way in which AI was used when formulating our response. **We will ensure that unethical or irresponsible use of AI is discovered, attributed and met with an appropriate response.**



The Schiebel's CAMCOPTER S-100 Uncrewed Air System (UAS) trialled during Ex UNCREWED WARRIOR. This exercise is part of ongoing experimentation, and demonstrates the use of autonomous systems, showing off the benefits that these potentially future capabilities will bring to the Royal Navy.

# 6. Strategy Implementation and Beyond

It is essential that all parts of our business are incentivised, motivated and resourced to respond to the challenges of AI at the required pace and scale. Defence is a complex organisation. **Each part will face its own unique combination of AI opportunities, issues and disruptions – and every part has a responsibility to rise to the challenge and contribute to the delivery of our vision.**

- All Functional Owners, Front Line Commands, Top Level Budgets (TLBs) and Enabling Organisations will provide a formal response to this Strategy within six months of publication;
- Building on these responses, leaders and organisations will either deliver a stand-alone AI strategy/plan or ensure that AI is prominently covered within other strategies and plans;
- Head Office will ensure that corporate, strategic and Functional plans align to this Strategy and set ambitious objectives and headmarks, and that the full range of issues set out in this document are suitably covered;
- All senior Committees and Boards will review their responsibilities and activities, providing formal assurance that they are aligned and coherent with this Strategy and any additional AI plans that emerge.

## 6.1 Priorities

Individual organisations and Functions will need to prioritise their activities as part of the process described above, overseen by Head Office. At the Defence level, our immediate priorities are to:

- Make immediate changes to the way we **structure our data** so that we start building the curated data-sets we need for AI adoption;
- **Deliver the Defence AI Centre (DAIC)** as an Initial Operating Capability, with particular emphasis on establishing effective links to industry and academia;
- Develop and embed our '**Ambitious, Safe, Responsible**' approach to AI in Defence, with Head Office leading on overarching policy and process, and UKStratComd leading more detailed work amongst the community of military practitioners and operators;
- Create and communicate **technology / programme roadmaps** and the first iteration of the **AI Technology Strategy** to guide project teams across Defence.



## Future facing: AI in a Smart Supply Chain

Defence Support have trialled and proved the value of tracking assets in the end-to-end supply chain with sensors. The next stage is to test technologies such as 5G to provide a core infrastructure capable of maximising the exploitation of this new vast array of data. We would know, at any one point in time, when an asset in the supply chain is missing or has gone (or is about to go) unserviceable or perish due to temperature. A Smart Supply Chain, needs to be Instrumented, Interconnected and Intelligent – underpinned by AI – to action this information and optimise the flow of goods, reserving operators' time for the most complex problems.

- **Instrumented:** Information that was previously created by people will increasingly be machine generated – flowing out of sensors, RFID tags, meters, actuators, GPS and more. Containers will detect their contents. Pallets will report in if they end up in the wrong place. This will be enabled by a 5G network.
- **Interconnected:** The end-to end supply chain will be connected – not just customers, suppliers, and IT systems in general, but also parts, products and other smart objects used to monitor the supply chain. Extensive connectivity will enable inter-operability between Allies and coalition partners networks of supply chains to plan and make decisions together.
- **Intelligent:** The supply chain decision-making will also be much smarter. Advanced analytics and modelling will help decision-makers evaluate alternatives against an incredibly complex and dynamic set of risks and constraints. And smarter systems will make appropriate decisions automatically, increasing responsiveness and limiting the need for human intervention.

## 6.2 Leadership and Governance

The **2<sup>nd</sup> Permanent Secretary** and the **Vice Chief of the Defence Staff** will oversee and drive activity across Defence. They will scrutinise and agree the responses and approaches described above, and own an overarching Defence AI Strategy Implementation Plan. This Plan will be informed by the outputs described above and will clearly map activities and responsibilities.

The **Defence Technology & Innovation Board** (DTIB) will serve as AI Strategy Implementation Board. 2<sup>nd</sup> PUS and VCDS, as co-chairs, will

scrutinise the activity of other senior boards and conduct an annual **AI Stocktake** through the DTIB. The technological and global context will evolve rapidly, our plans will become more detailed, we will learn lessons about the efficacy of our approach, and AI will become a more prominent part of ‘business as usual’ activities. To ensure these changes and opportunities are appropriately reflected in high-level direction, and to maintain momentum, the DTIB will oversee a refresh of this Strategy (led by the Defence AI & Autonomy Unit), accompanied by a review of plans across Defence organisations, after two years.

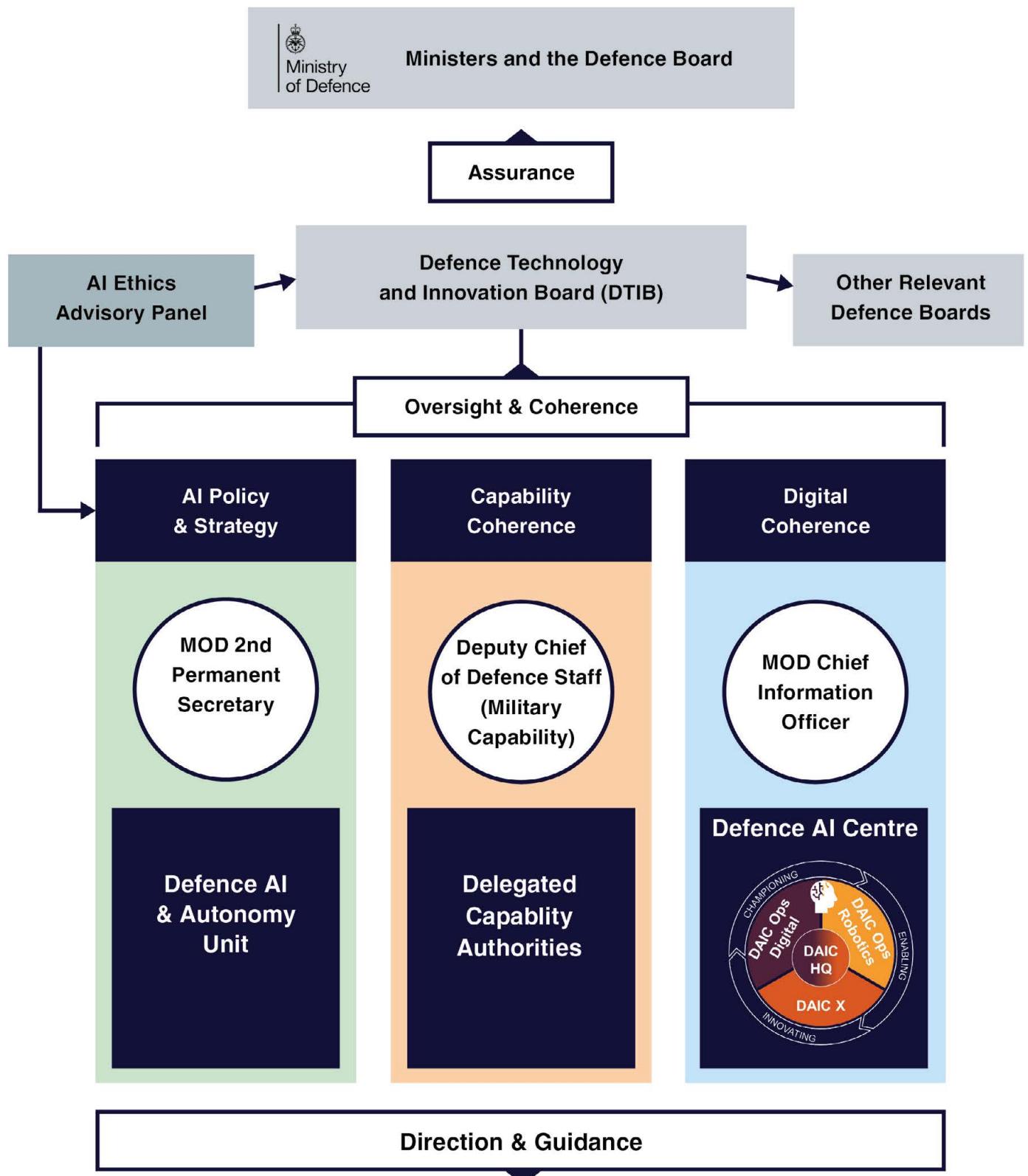
## 6.3 Looking Ahead

**To become a truly ‘AI Ready’ organisation – and to go beyond that and become ‘AI pre-eminent’ – senior leaders and personnel right across the organisation must proactively and creatively drive change, with the following principles particularly in mind:**

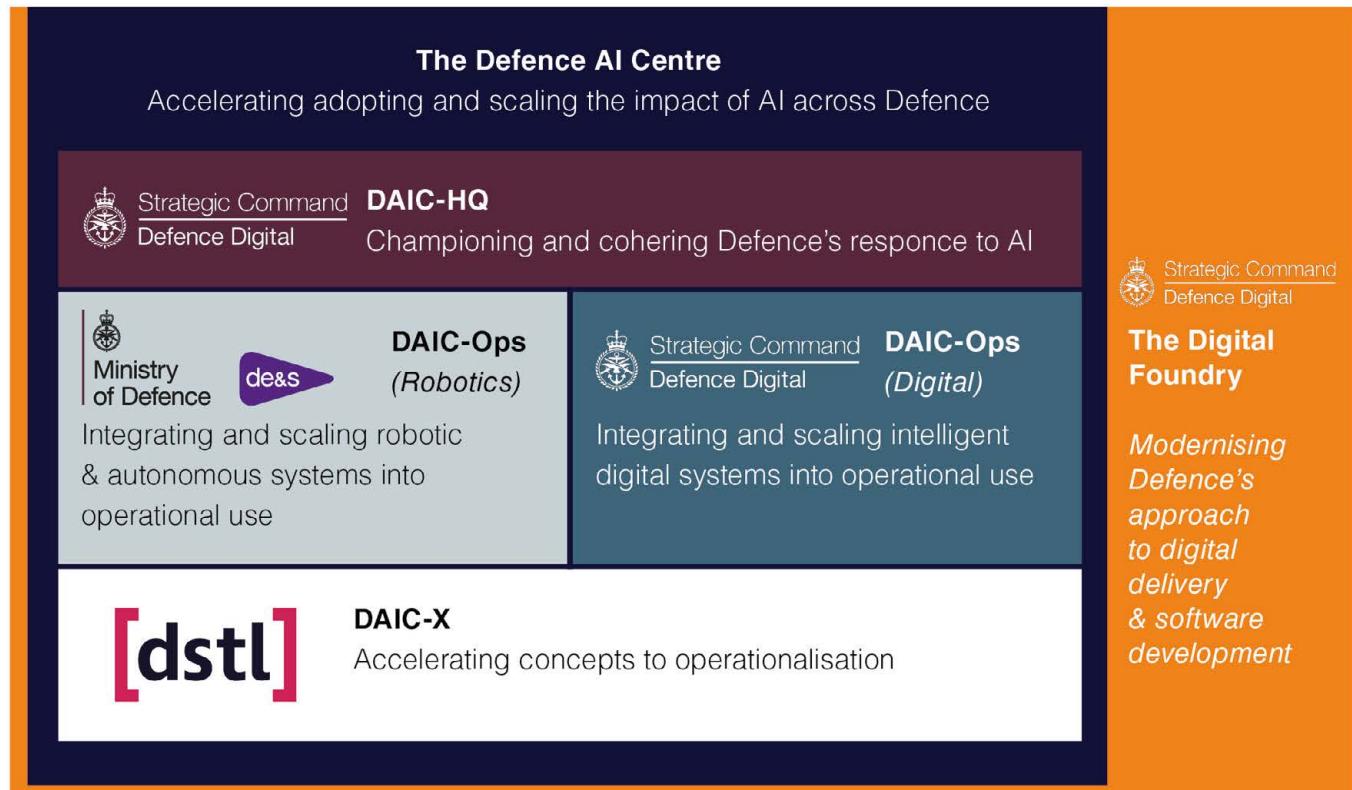
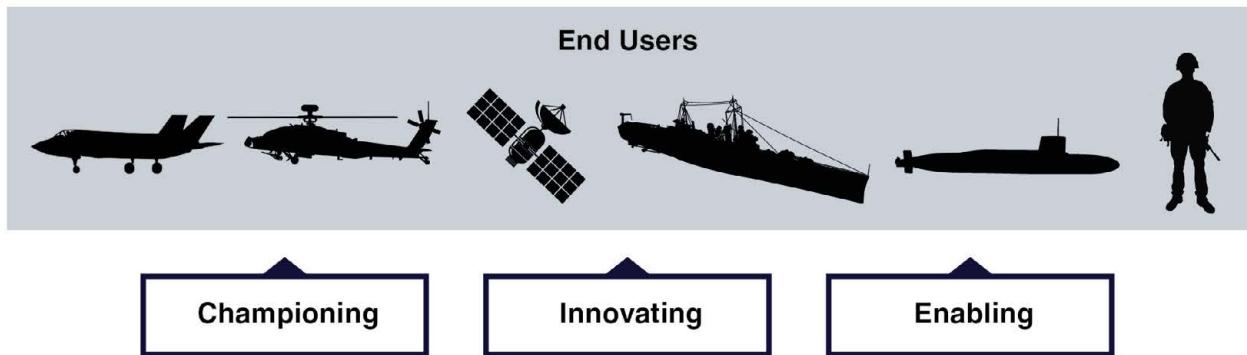
- We must fundamentally change the way we think about modern technology. It is not merely an enabler, but a powerful disruptive and creative force. We cannot isolate ourselves from these effects, which only partly relate to our own choices around adoption and exploitation. Nations that embed technological understanding and strategic insight at the heart of their decision-making and plans will have a decisive advantage;
- AI must be the essential future technology for almost everything that we do. We must be ambitious, aiming to deliver world-leading AI solutions and AI-enabled capabilities;

- We must be prepared to adjust our world-view and learn to value different things, particularly our data and the speed and quality of insights we can gain from it;
- National ‘science power’ underpins all facets of our security, prosperity and international influence. We have a strategic interest in the long-term health and resilience of the national tech sector, and an important role in ensuring UK R&D policies and activities – from security to trade and diplomacy – support that long-term future;
- We must change the way we think about the nature of work, the skills that our people need and the way we organise for success.
- **Everyone in Defence has a stake and role in this change. We must catalyse an enduring change in mindset, culture, planning and delivery at all levels and across all parts of our organisation.**

# Annex A: AI Governance in Defence



# Annex B: The Defence AI Centre

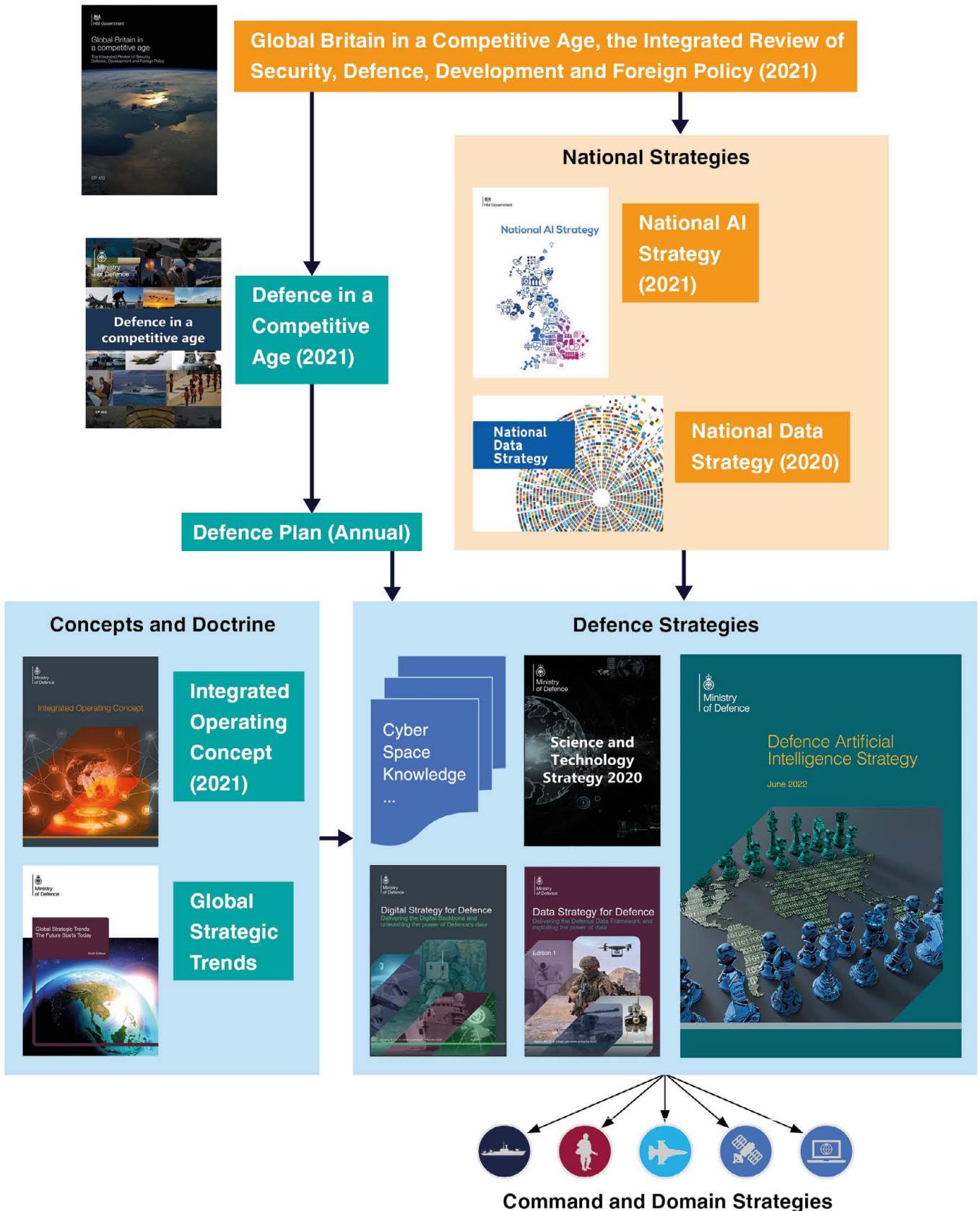


**DAIC Partners**  
Prototype warfare & user-led experimentation (FLC led)

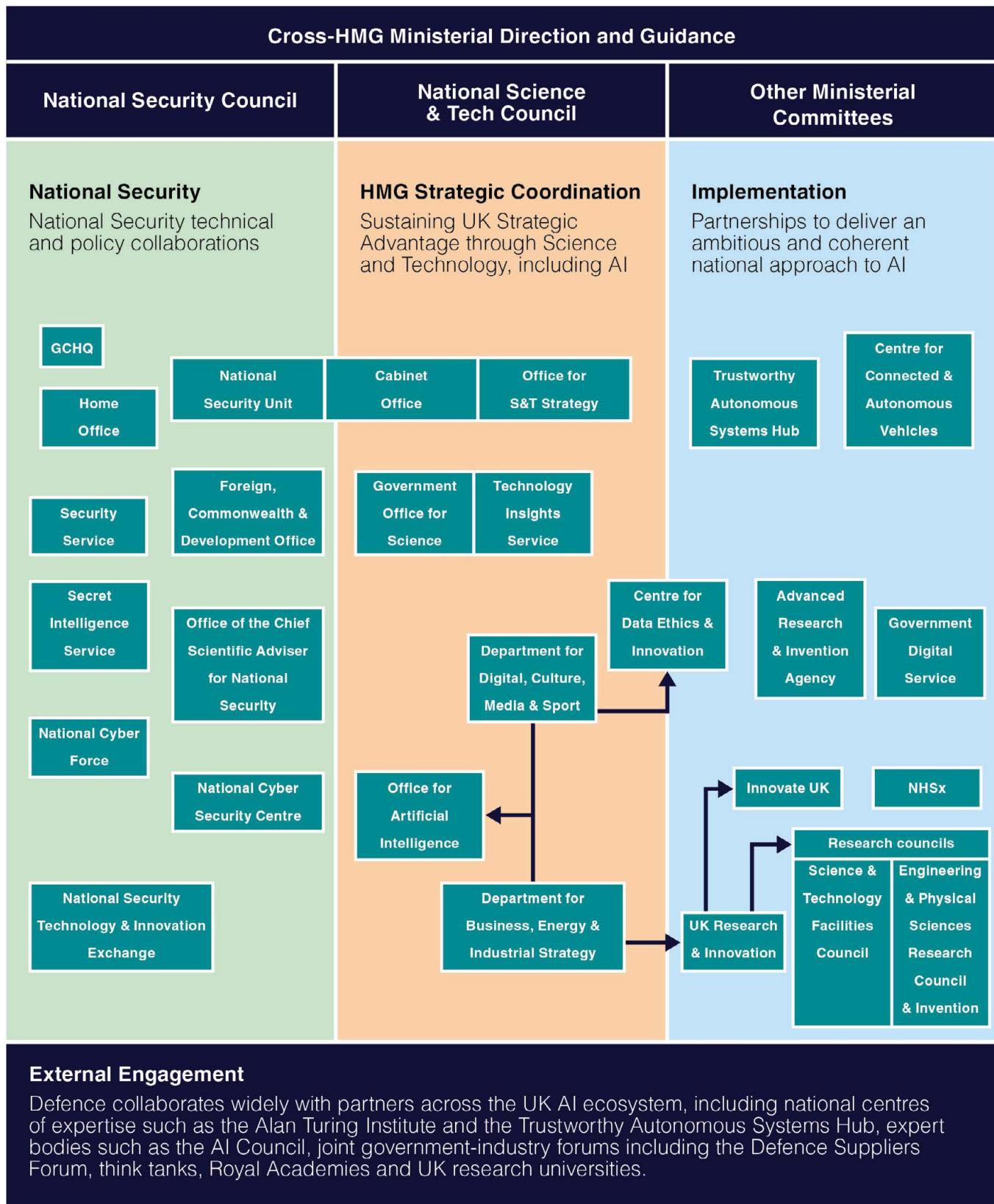
**Industry, Academia, Allies & Partners**



# Annex C: Strategic background



# Annex D: Defence national engagement on AI



# Endnotes

- [1] The Integrated Review (2021) - [www.gov.uk/government/collections/the-integrated-review-2021](http://www.gov.uk/government/collections/the-integrated-review-2021)
- [2] National AI Strategy (2021) - [www.gov.uk/government/publications/national-ai-strategy](http://www.gov.uk/government/publications/national-ai-strategy)
- [3] The Integrated Operating Concept 2025 (2020, updated 2021) - [www.gov.uk/government/publications/the-integrated-operating-concept-2025](http://www.gov.uk/government/publications/the-integrated-operating-concept-2025)
- [4] Defence in a Competitive Age (Defence Command Paper) (2021) - [www.gov.uk/government/publications/defence-in-a-competitive-age](http://www.gov.uk/government/publications/defence-in-a-competitive-age)
- [5] Digital Strategy for Defence (2021) - [www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data](http://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data)
- [6] Data Strategy for Defence (2021) - [www.gov.uk/government/publications/data-strategy-for-defence](http://www.gov.uk/government/publications/data-strategy-for-defence)
- [7] The UK AI Ecosystem encompasses everything from early-stage science and research, regulators and standard setting bodies, through to entrepreneurs, SMEs and large-scale high-tech manufacturing capabilities.
- [8] Defence and Security Industrial Strategy (2021) - [www.gov.uk/government/publications/defence-and-security-industrial-strategy](http://www.gov.uk/government/publications/defence-and-security-industrial-strategy)
- [9] The Data City, UK Artificial Intelligence analysis (2020) - [thedatacity.com/insight/uk-artificial-intelligence-analysis-2020](http://thedatacity.com/insight/uk-artificial-intelligence-analysis-2020)
- [10] TechNation Report (2021) [techn nation.io/report2021/#global-capital-flows](http://techn nation.io/report2021/#global-capital-flows)
- [11] Technology Unicorns are defined as new privately-owned businesses with a value of more than \$1bn
- [12] Tortoise Media Global AI Index (2021) - [www.tortoisemedia.com/intelligence/ai](http://www.tortoisemedia.com/intelligence/ai)
- [13] Global AI Talent Tracker (2021) - [macropolo.org/digital-projects/the-global-ai-talent-tracker](http://macropolo.org/digital-projects/the-global-ai-talent-tracker)
- [14] Ambitious, Safe, Responsible, MOD Policy Statement, June 2022
- [15] The Centre for Data Ethics & Innovation is a government expert body enabling the trustworthy use of data and AI. It is part of the Department for Digital, Culture, Media, and Sport - [www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about](http://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about)
- [16] The Office for Artificial Intelligence is a joint Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy unit responsible for overseeing implementation of the National AI Strategy - [www.gov.uk/government/organisations/office-for-artificial-intelligence/about](http://www.gov.uk/government/organisations/office-for-artificial-intelligence/about)
- [17] Digital, Data and Technology Profession Capability Framework (2020) - [www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework](http://www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework)
- [18] MOD Science and Technology Strategy (2020) - [www.gov.uk/government/publications/mod-science-and-technology-strategy-2020](http://www.gov.uk/government/publications/mod-science-and-technology-strategy-2020)
- [19] The Defence Data Framework, Data Strategy for Defence (2021) - [www.gov.uk/government/publications/data-strategy-for-defence/data-strategy-for-defence#the-defence-data-framework](http://www.gov.uk/government/publications/data-strategy-for-defence/data-strategy-for-defence#the-defence-data-framework)
- [20] 'Beyond CMOS' refers to possible future technologies not limited by heat-related CMOS scaling limits typical for Complementary Metal-Oxide Semiconductors
- [21] Such as the Alan Turing Institute ([www.turing.ac.uk](http://www.turing.ac.uk)), Trustworthy Autonomous Systems Hub ([www.tas.ac.uk](http://www.tas.ac.uk)) and Assuring Autonomy International Programme ([www.york.ac.uk/assuring-autonomy](http://www.york.ac.uk/assuring-autonomy))
- [22] These capability challenges are described in the MOD S&T Strategy (2020), reflecting how we need to adapt in line with the Integrated Operating Concept 2025
- [23] US DoD FY2021 Budget Request - [comptroller.defense.gov/Budget-Materials/Budget2021/](http://comptroller.defense.gov/Budget-Materials/Budget2021/)
- [24] Summary of the NATO Artificial Intelligence Strategy (2021) - [www.nato.int/cps/en/natohq/official\\_texts\\_187617.htm](http://www.nato.int/cps/en/natohq/official_texts_187617.htm)
- [25] Stanford University, Artificial Intelligence Index Report 2021 (2021) - [hai.stanford.edu/research/ai-index-2021](http://hai.stanford.edu/research/ai-index-2021)
- [26] The NSSIF is the government's corporate venture arm for dual-use advanced technologies. It invests in technology companies whose product and services have the potential to be adopted by national security and defence customers to deliver improved capabilities - [www.british-business-bank.co.uk/national-security-strategic-investment-fund](http://www.british-business-bank.co.uk/national-security-strategic-investment-fund)

- [27] Opportunity & Innovation: The Defence Small and Medium-sized Enterprise (SME) Action Plan (2022) - [www.gov.uk/government/publications/opportunity-and-innovation-the-defence-small-and-medium-sized-enterprise-action-plan](http://www.gov.uk/government/publications/opportunity-and-innovation-the-defence-small-and-medium-sized-enterprise-action-plan)
- [28] Defence Technology Framework (2019) [www.gov.uk/government/publications/defence-technology-framework](http://www.gov.uk/government/publications/defence-technology-framework)
- [29] Financial Conduct Authority Digital Sandbox <https://www.fca.org.uk/firms/innovation/digital-sandbox>
- [30] A range of government incentives schemes are set out in the HMG Innovation Strategy (2021) - <https://www.gov.uk/government/publications/uk-innovation-strategy-leading-the-future-by-creating-it>



Ministry  
of Defence