Ministry
of Defence

Data Strategy for Defence

Delivering the Defence Data Framework and exploiting the power of data

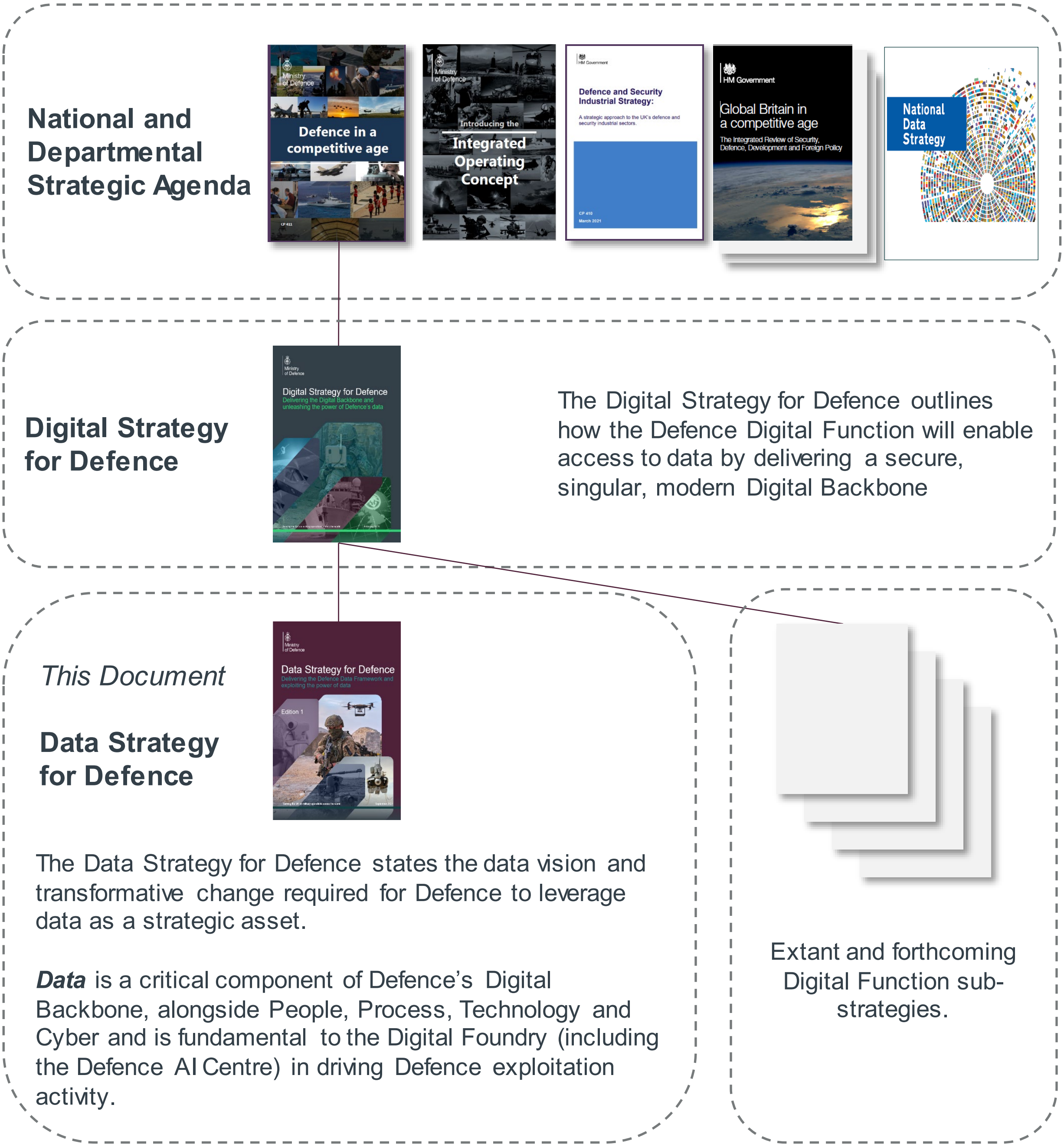
Edition 1

Serving the UK on military operations across the world

September 2021

Map to the Digital Strategies

The Data Strategy for Defence should be read in conjunction with the Defence Integrated Review Command Paper “Defence in a Competitive Age”, the Digital Strategy for Defence and extant and forthcoming Digital Function sub-strategies. See Annex B for a wider view of strategies and policies that have driven the development of this strategy.


Defence in a competitive age
Introducing the Integrated Operating Concept
Defence and Security Industrial Strategy:
Global Britain in a competitive age
National Data Strategy
Digital Strategy for Defence
Data Strategy for Defence

National and Departmental Strategic Agenda

Digital Strategy for Defence

The Digital Strategy for Defence outlines how the Defence Digital Function will enable access to data by delivering a secure, singular, modern Digital Backbone

This Document

Data Strategy for Defence

The Data Strategy for Defence states the data vision and transformative change required for Defence to leverage data as a strategic asset.

Data is a critical component of Defence’s Digital Backbone, alongside People, Process, Technology and Cyber and is fundamental to the Digital Foundry (including the Defence AI Centre) in driving Defence exploitation activity.

Extant and forthcoming Digital Function sub-strategies.

Placing the Data “Rules of the Road” for Defence at the heart of its approach, the Data Strategy for Defence matches the Defence Data “Ends” with the “Ways” and “Means” required to deliver on Defence Outcomes in a competitive information and technological age, through exploitation of data.

Data Strategy for Defence – on a page

1. *Diagnosis: The Data challenges in Defence are understood*

Despite a rising volume of data from our increasing arsenal of sensors, we're finding it harder than ever to isolate the insight from the information. This is Defence's data paradox.

- Data is inaccessible in internal or contractual silos
- Lack of recognition that data is important
- Critical data skills gaps and lack of accountability for data
- Non-standardised exploitation and data delivery
- Inconsistent governance and control
- Overlapping data holdings across Defence

The Defence data transformation has commenced, a central Data Office, part of Defence Digital has been established as well as a Defence Data Framework to transform Defence's culture, behaviour and data capabilities. Data will be the horizontal enabler that will optimise operational and business outcomes, informing better, faster decision-making and command and control, nationally and internationally, across all five domains and with our partners across government, allies and industry.

2. *Ends: The end state, with clear strategic outcomes for Data by 2025, is defined*

Vision: Defence Data is an enduring strategic asset, effectively exploited and driving sustainable battlespace advantage and business efficiency.

Strategic Outcomes: ***where will Data in Defence be by 2025***

Data is curated, integrated and human and machine ready for exploitation – Data enables digitalisation of the battlespace

Data is treated as the second most important asset only behind our people – Data is considered in all Defence activities

Our people are skilled and exploiting data to drive advantage – Defence people are data-literate and optimising exploitation

Defence are data leaders with partners, allies and industry – Defence drives innovation with partners, allies and industry on data

3. *Ways: Defence will adhere to, and be measured against explicit data rules*

The Data Rules set out how Defence must treat data and how all of Defence will adhere to the same data criteria. The rules provide the basis for a future connected Defence enterprise, underpinned by a business model optimised for data exploitation. All data delivery programmes and decisions across Defence will be measured and assured against these.

Exercise ***sovereignty*** over data, including accountability and ownership

Standardise data across the Defence landscape

Exploit data at the most effective and relevant point in the value chain

Secure digital data at creation, curation, when handling, storing and transmitting

Curate data, ensuring it is assured, discoverable and interoperable

Endure data as an asset beyond individual projects

4. *Means: Key success factors are required to enable and facilitate this paradigm shift*

Enablers: required to transform Defence into an enduring data driven enterprise, empowering our people to exploit data for advantage, and have the means to adhere to the rules

Organisation – Central leadership driving Defence's functional data mandate; central and local teams working together to deliver the data vision

People, Skills and Culture – Modernising Defence through adoption of a digital and data driven culture, investing in developing data skills

Governance and Controls – Embedding governing structures and data controls that ensure Defence does not overlook data

Data Foundations – Defence's priorities drive standards, practices and policies to preserve and enhance the value of data

Exploitation – Optimising data that is ready for exploitation through a common framework; sustaining and evolving Defence's exploitation efforts

Facilitators: required to co-ordinate and facilitate the execution of the strategy by establishing and embedding the data enablers.

Funding – a sustained funding approach across Defence to develop and curate exploitable data assets, as well the expertise to exploit these assets

Plan – a pan-Defence plan with delivery milestones to track progress

Measures – Specified and baselined measures to track delivery on strategic data intent

The Transformation of Data in Defence

"The victors of the future will be those who are able to master data and new technology."

Rt Hon Boris Johnson MP, Prime Minister

Data has always contributed to success in Defence, it's fast becoming our lifeblood. Every decision we make is increasingly data-driven; from multi-billion pound investment and divestment choices, to life-or-death situations handled in a split second on the battlefield, to defending against the increasing volume of cyber threats.

Despite a rising volume of data from our increasing armoury of sensors, we're finding it harder than ever to isolate the signal from the noise. This is Defence's data paradox.

We have wonderful exemplars of data-driven practices in Defence, take Project Kraken's situational awareness platform, which allowed the First Sea Lord to exploit data on his workforce to effectively support the Covid-19 pandemic response, but these exemplars are rare. They're outnumbered by:

- reports from a senior leader that has to make critical decisions based on intuition and not insight;
- the pilot who has to use an excel spreadsheet to calculate where to drop our high altitude parachutists as opposed to information being auto-derived from a variety of trusted data sets; and
- the intelligence analyst trying to glean insights from 500Gb of data from captured enemy material by manually scrolling through it in a spreadsheet, fruitlessly trying to find the needle in the haystack.

It is perhaps not surprising that we suffer this paradox. Our data landscape is complex. In a recent review of 100 Defence systems, it was identified that just 25% of our systems have data that is automatically discoverable (requires minimal manual intervention). Our specialist skills are limited and we are an increasingly frustrating partner for allies, other government departments and industry who struggle to share data with us. Put simply, we are a data laggard.

The Defence Data Strategy establishes a strong stake on the ground and sets precedent to resolve Defence's own data paradox. In a world of exponentially increasing data, the Strategy mobilises Defence to cohere in service of enabling systems interoperability and adequate channelling of investment into the right capabilities and tools to enable data sharing and insight at the point of need. Given unprecedented global uncertainty, threats across multiple domains, and the increasingly digital arms race - every soldier, sailor, aviator, analyst is going to need these insights.

This Strategy outlines four outcomes: data is ready for exploitation; data is treated as the second most important asset only behind our People, our people are appropriately skilled to exploit it; and, through a culmination of these first three outcomes and partnership with others, Defence becomes a global Data Leader. This Strategy captures these ends and describes the ways and the means by which they will be delivered. Whilst there is a long way to go before Defence achieves the status of Data Leader, it should be an unashamed ambition of every member of Defence Personnel. Our status as a 'victor' as the Prime Minister puts it, will increasingly depend upon it.

Laurence Lee, Second Permanent Secretary – Ministry of Defence

Our ambition to '*unleash the power of data*' is stronger than ever. Our future will be shaped by how we protect and exploit Defence's assets. Data will become our second most important asset only behind our People. This is the clear intent of our Data Strategy. It describes the journey, and the part we must all play in living by the "rules of the road" to effect this change across Defence. It is our people, our communities and our nation that will benefit from Defence's transformation to a data-centric connected enterprise.

Charles Forte.

Charles Forte, MOD Chief Information Officer, Digital Functional Lead

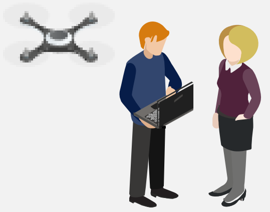
Unleashing the power of Defence's data

As Defence's curated data starts to flow seamlessly between users and across platforms, a truly connected Enterprise will deliver integration, nationally and internationally, across all five domains: Maritime, Land, Air, Cyber and Space. This will enable Defence to fully unleash the power of its data, connecting sensors, decision makers and effectors at scale and speed.

*"We urgently need to invest in the technologies that will revolutionise warfare. In the future a soldier in hostile territory will be alerted to a distant ambush by sensors on satellites or drones, instantly transmitting a warning, using Artificial Intelligence to devise the optimal response, and offering an array of options, from summoning an air strike to ordering a swarm attack by drones, or paralysing the enemy with cyber weapons." - **Rt Hon Boris Johnson MP, Prime Minister***

Sensors	Decision makers	Effectors
detect a physical or digital signal	decide on the best course of action	respond to signals as per the decision

The below present example scenarios for Defence to drive battlespace advantage and business efficiency through exploiting its data in a multi-domain and integrated environment.

	Sensors	Decision makers	Effectors
Last mile logistics	*Radio batteries self-report low battery load. Via soldier's C2 system, commander and logistical support team are informed immediately.* 	 *The logistical support are provided with real-time data to trigger immediate re-supply action.*	*Radio batteries delivered by unmanned air asset to ground systems, planned via automated Mission Management & Asset Planning capabilities and controlled by automated Unmanned Asset Command and Control (C2).*
Political demonstration	 *Automated scanning of social media platforms (analysing key words and interactions) detects change in population sentiment.*	*Local authorities are quickly informed of change in sentiment. Decision making is enhanced by local surveillance of groups of interest.* 	 *Escalated monitoring and intelligence gathering, with heightened readiness measures to respond in place.*

Additional examples along with further information on the Last Mile Logistics challenge can be found in Annex C.

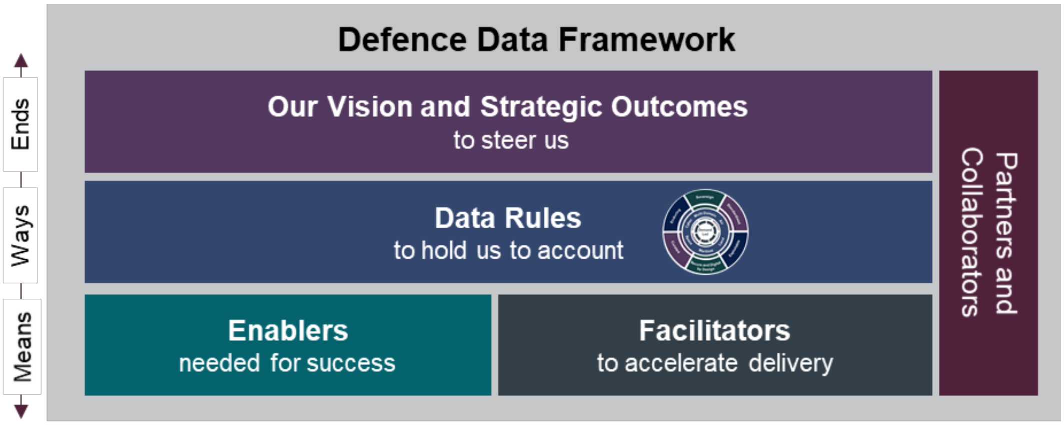
Preface

Purpose

The purpose of this Data Strategy for Defence is to state the data vision and transformative change required for Defence to leverage data as a strategic asset. Defence must capture, curate, share and exploit data more effectively and consistently pan-Defence to deliver better decisions and outcomes. Mastering data will require a paradigm shift in behaviour and culture. Only when Defence is able to achieve this will it secure battlespace advantage and business efficiency.

The strategy articulates the strategic outcomes, data rules and common foundations to ensure data becomes a horizontal enabler and an enduring capability across Defence. It formalises the functional leadership for data and how it will be asserted to cohere Defence as a global enterprise.

Placing a Data Framework at the heart of the approach, this strategy describes what needs to be in place to build and deliver the framework and enable and accelerate exploitation across Defence. The strategy aligns Ways with the Means required to deliver the Defence's Data Ends. Defence needs to invest in data, particularly changing behaviours and culture and developing data skills, if it is to transform and compete in the digital age. This is a Defence wide Data Strategy, reaching beyond the Defence Digital function.



Audience

The strategy provides clear intent, direction and guidance for all across Defence – Functions, Commands and Enabling Organisation. All personnel, irrespective of rank, have a role to play in transforming data to become a strategic asset.

This strategy is aimed at a broad readership including users, owners and stewards of data, decision-makers and partners across government, international allies and industry. The strategy will be of particular interest to members of the Defence Information Steering Committee (DISC), the Strategic Data Committee (SDC) and the Steering Data Strategic Group (SDSG).

Defence Data Rules Overview

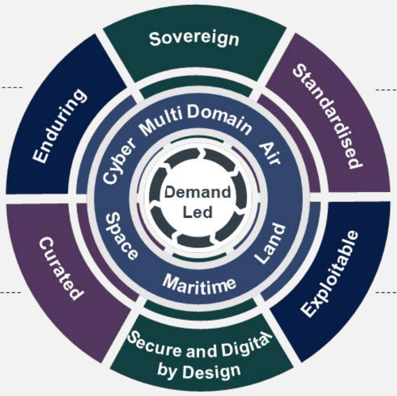
The Defence Data rules set out how Defence will treat data to become a connected enterprise. All programmes and activity will need to demonstrate compliance with these rules and will be assured against these.

The six Data Rules Defence must apply:

1. Exercise *sovereignty* over data, including accountability and ownership
2. *Standardise* data across the Defence landscape
3. *Exploit* data at the most effective and relevant point in the value chain
4. *Secure digital* data at creation, curation, when handling, storing and transmitting
5. *Curate* data, ensuring it is assured, discoverable and interoperable
6. *Endure* data as an asset beyond individual projects

Sovereign

Defence knows what data it has, where it is, how it is used, sets its policy and is able to assure its adherence to it, regardless of who has custody of it.



Enduring

Data is an enduring asset and capability. It persists beyond the life of a project and is continuously maintained to drive military and functional exploitation.

Standardised

Defence follows Industry, Government, Data Management, and Technical standards. The Defence Data Framework provides the artefacts and methods to be applied across Defence in a cohered manner.

Curated

Data is assured, discoverable, interoperable. It is separate from platforms and is always aligned to the Defence Data Framework and Standards.

Exploitable

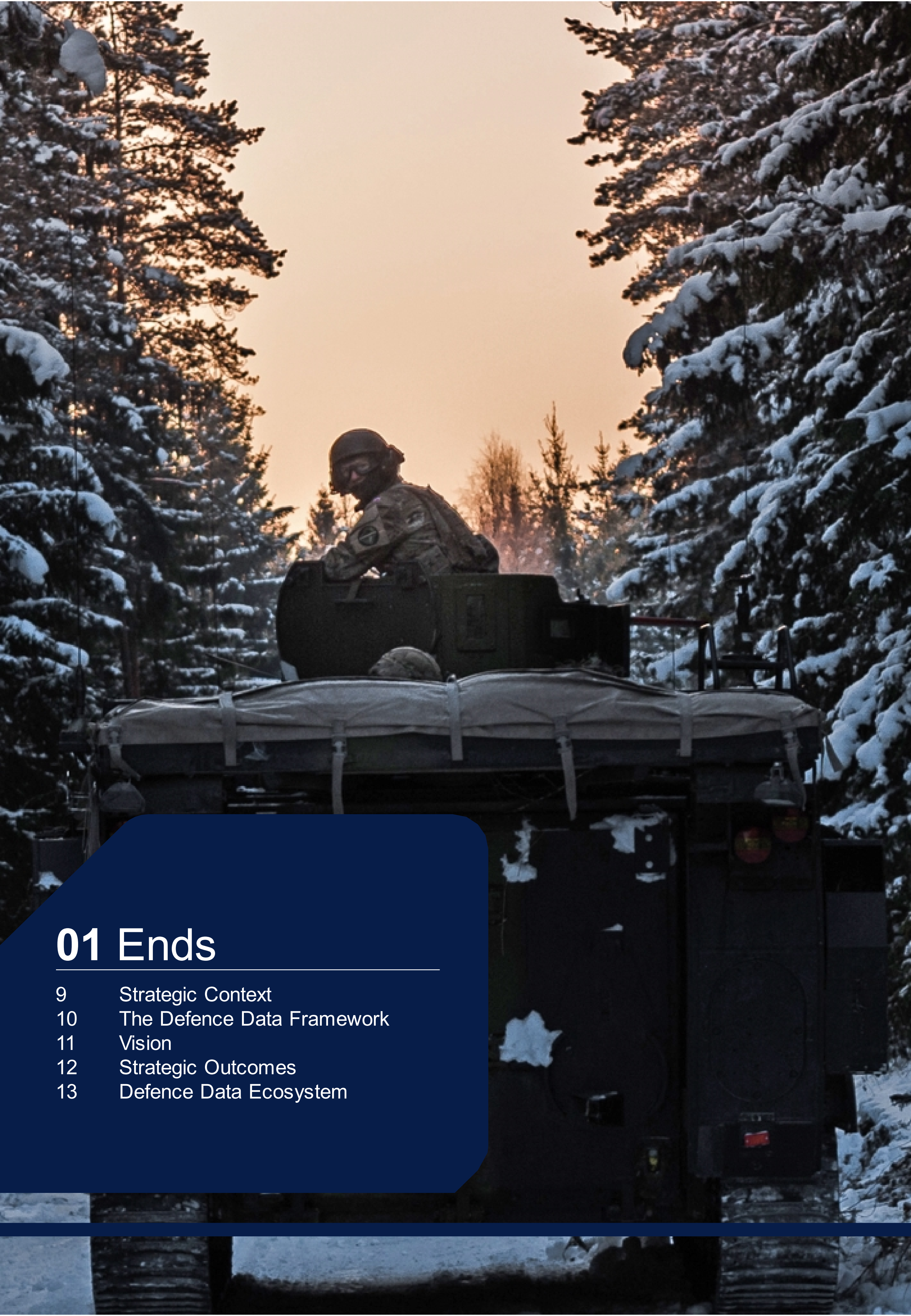
Defence operates a frictionless business model that enables exploitation at the most effective and relevant point in the value chain (e.g. close to the customer through self-serve).

Secure and Digital by Design

Defence Data is robust, fit for purpose, trusted and secure in a digital format. Data complies with legal, regulatory and ethical obligations.

Further information on the Defence Data Rules and how Defence will live up to the rules can be found in Ways section of this Data Strategy for Defence.

Contents



01 Ends

Strategic Context

The Defence community operates in an information age of rapid technological change, increasing competition and new threats to our national security. These changes also present new opportunities with the potential of greater integration, sharing and exploitation of data. Realising the material advantage from these opportunities; however, is dependent on the availability of accurate, relevant and interoperable data.

The importance of data therefore can no longer be ignored nor undervalued. Defence must transform from a "need to know and platform centric" conglomerate to a "need to share and data-centric" connected enterprise.

Facing unprecedented global uncertainty, Defence must adapt to become insightful, effective and proactive against adversaries that threaten the United Kingdom. Adversaries are changing, in terms of who they are and how they fight, undermining the international rules-based order by competing in ways that do not necessarily involve military confrontations. Advances in Science and Technology present both threats (as adversaries are exploiting them today) and also opportunities (for us to exploit and use to our advantage). Therefore, the distinction between war and peace has become increasingly blurred.

Other threats include terrorism, biosecurity risks and hyper-sonics. Against this backdrop, there are other political imperatives associated with the COVID-19 pandemic, climate change, the 'levelling up' agenda to strengthen the Union and promote UK prosperity, which compel Defence to change now. The UK's traditional military advantage has therefore been eroded.

> *"The future performance in war will be dominated by the relentless and competitive exploitation of data: undersea, on the sea, in the air and in space. All together."*
>
> ***Sir George Zambellas, Former First Sea Lord, Royal Navy***[1]

Exploiting data is critical to achieving military and business advantage. In the face of public spending pressures, we must act to prioritise and maximise Defence's data investment. Defence faces similar data challenges applicable to other government departments outlined in NAO Report - Challenges in using data across government. These clear challenges will be addressed as follows:

- **Defence data operates in contractual, technical and behavioural silos** – Ownership and control mechanisms are required across organisations in order to facilitate a common view on the availability, quality and location of data across Defence.
- **Defence has a complex business model with unclear accountabilities, presenting additional challenges for data curation and exploitation** – Organisations will need to define and enforce clear accountability and have governance and control mechanisms to enforce them.
- **Culturally, Defence lacks recognition over the importance of data** – All personal across levels and organisations must dedicate effort to better use data and have a responsibility to adhere to common data standards and practices. This will be enabled by the enforcement of data governance, controls and management practices across Defence.

Given the data challenges and consequences, Defence must act now and avoid further problems. This strategy sets out the mechanisms for Defence to address these challenges, in collaboration with the forthcoming Defence AI centre, a subset of the Digital Foundry.

[1] Stated 2016

The Defence Data Framework

The Defence Data Framework provides a structure to address the challenges and transform Defence's culture, behaviour and data capabilities to align with a data-driven enterprise. The framework establishes a unified strategic direction for data for all Defence personnel to align to and play a proactive role in building and adhering to it. The Defence Data Office (DDO), part of Defence Digital (DD) will cohere Defence into delivering the framework.

The Defence Data Framework comprises of:

Vision and Strategic Outcomes **–** A data vision for all of Defence and key outcomes setting the direction for the future of data in Defence.

Data Rules **–** Defining what Defence data will look like in future. Data rules are expected to be understood, promoted and adhered to by everyone in Defence to achieve the vision for data.

Enablers **–** Required to transform Defence into an enduring data driven enterprise, empowering our people with the means to adhere to the rules.

Facilitators **–** The supporting mechanisms required to co-ordinate and facilitate the execution of the Strategy by establishing and embedding the Enablers. These include the delivery funding, plan and measures.

Partners and Collaborators **–** Critical partnerships to collaborate and cohere within Defence and across the wider data ecosystem with allies, industry, agencies and academia.

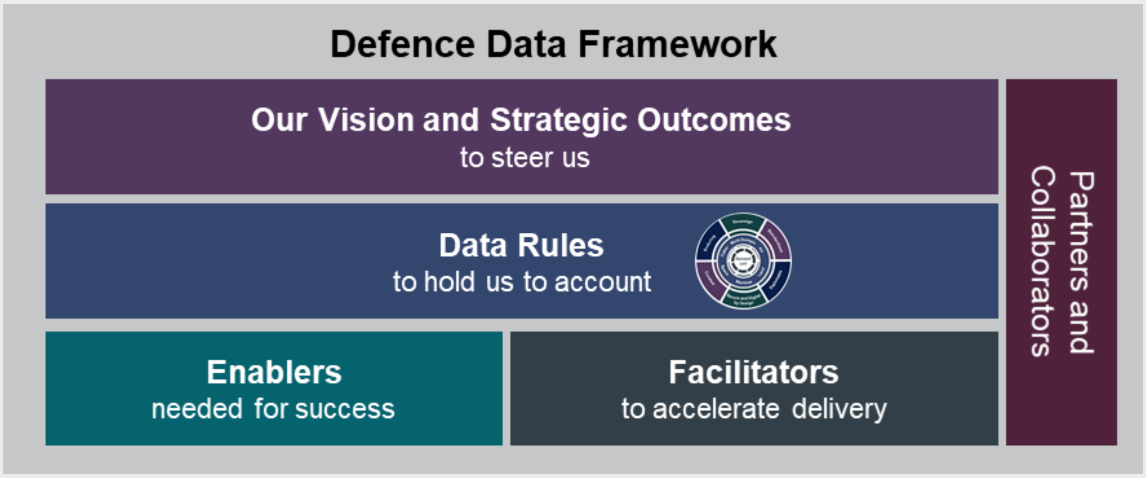


Figure 1 – The Defence Data Framework to transform Defence to become a digitally enabled organisation

Vision

Our Vision: *Defence Data is an enduring strategic asset, effectively exploited and driving sustainable battlespace advantage and business efficiency.*

We will become an organisation that recognises, manages and exploits data for what it is: ***a Defence Strategic Asset.*** To achieve our vision:

Defence will recognise data as a strategic asset, second only to our people. Data will be recognised and treated as strategically in the same manner that Defence treats its people, weapons and equipment. This recognition will also apply to non-Defence generated data for the value and contribution it brings and the partnerships it forms. This will require a paradigm shift in our data culture, behaviours and skills towards championing the data theme and raising its profile across Defence and with partners, allies, industry and academia.

Defence data will be maintained as an asset. Data will be continuously managed and maintained so Defence Organisations, programmes and capabilities within business and the battlespace have data available and accessible that is fit for purpose to exploit. All data, generated within or outside Defence, has transformational value beyond Defence boundaries, enabling opportunities, such as driving a new era of growth and improving public services as set out in National Data Strategy[1].

Defence will maximise value from its data. Defence will create the digital environment where data is integrated and democratised to niche and pan-Defence requirements. From driving analysis for operational and business decision making, to enabling delivery of the Science and Technology vision and strategy; it is the exploitation of data, at every level, across every organisation, that will revolutionise warfare and modernise Defence.

This will allow us to derive maximum value through:

✓ Faster decisions and insights supported by exploitation of available and trusted data; enabling the frontline forces to have real-time access to data for faster situational awareness and decision making.

✓ Efficient and effective planning of supply chain and people. Organisation-wide integrated data will ensure functions and operations are reliably informed.

✓ Transforming operational capability - "the right sensors, effectors and decision-makers connected at the right time and place to deliver effect".

✓ Well curated data, directly enabling information, operations, analysis, analytics, AI and R&D, making it an offensive and defensive weapon.

✓ Optimising and accelerating programmes and transformations. Seamless data flow across the organisation through common technology, architecture and systems will enable data re-use and accelerated exploitation.

✓ Securing UK's status as a Global Science Power – by enabling delivery of the S&T vision and strategy, driving every idea or concept through scientific and evidence-based investigations, into a successfully deployed capability.

[1] National Data Strategy – Updated 9 December 2020

Strategic Outcomes

The Defence Data Strategic Outcomes outline Defence's ambition for its data by 2025. Defence Organisations must cohere their efforts to deliver the Defence data vision, changing how they currently operate, and taking the necessary actions to move towards enduring and exploiting their data.

Strategic Outcomes by 2025	Description	Achieved when
Outcome 1: Data is curated, integrated and human and machine ready for exploitation	Defence has a common approach to all aspects of data, complying with the data rules. Defence has resilient and secure data, available to those who need it, ready for interrogation and exploitation, driving better decisions.	Battlespace is digitalised, with curated data being the horizonal enabler across Defence.
Outcome 2: Data is treated as the second most important asset only behind our people	Data is seen as the lifeblood of Defence, recognised alongside people, weapons and equipment, through a culture and behaviour shift. Data is considered in all Defence activities.	Defence Organisations have well-structured and organised data functions and governance, better at funding, managing and maintaining the enduring value of data.
Outcome 3: Our people are skilled and exploiting data to drive advantage	All Defence people are data-literate and readily exploiting data to drive operations and make better decisions. There is an inclusive and diverse workforce who have a range of digital skills.	Exploitation practices are enabling the right sensors, effectors and decision-makers to be connected, delivering effective advantage at the right time and right place.
Outcome 4: Defence are data leaders with partners, allies and industry	Defence works and collaborates on data with partners, allies and industry to secure operational data access and drive innovation. Business, commercial and partner relationships are benefiting Defence through leveraging and contributing to exemplar mechanisms and platforms.	Defence is leading strategic data partnerships with key collaborators; becoming the centre of data expertise with international allies.

These strategic outcomes will be achieved through the adoption and implementation of a coherent, cross-cutting approach to data pan-Defence. The Defence Data Framework provides such an approach, mobilising Defence with a clear strategic intent.

Defence Data Ecosystem

Within Defence Organisations

The Data Strategy for Defence is aligned to the Digital Strategy for Defence. The Digital Strategy for Defence outlines a step-change in approach that is required for Defence to leverage digital and data as enablers to facilitate faster, better decisions and improved Defence outcomes.

As a critical enabler of Defence's Digital Backbone along with people, process and technology, adequate access to data enables Defence to connect internally and externally for interoperability. Data is a key customer and driver of technology, with more information available in the Digital Strategy for Defence.

Data's role in the continuous delivery of the Digital Backbone for a singular, secure, modern and digital environment, makes data itself a key enabler of the wider agenda for Multi-Domain Integration (MDI) and to realise the Integrated Operating Concept (IOC).

The Data Strategy for Defence seeks to cohere the Defence Organisations on a common agenda for the governance and management of data as an enterprise asset. Furthermore, data is a common denominator that is widely acknowledged by Defence Organisations and their strategies as an enabler for the delivery of their strategic objectives (for example, the Defence AI Strategy (document in production)). Data aims to optimise their operations, accelerate the introduction and use of digital solutions and to upskill and develop their people. This strategy will therefore align and support their narratives.

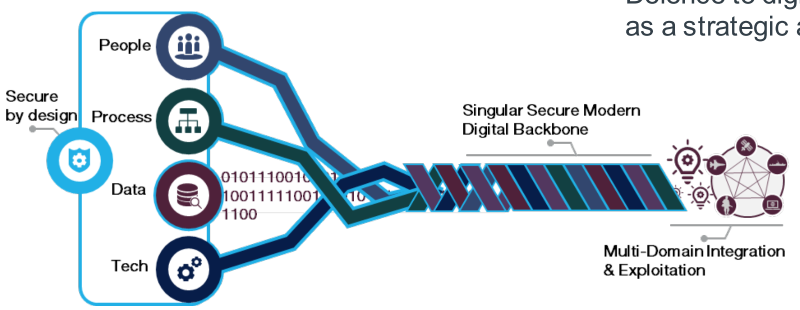

People
Secure by design
Process
Data
Tech
Singular Secure Modern Digital Backbone
Multi-Domain Integration & Exploitation

Figure 2 - The Digital Backbone Ecosystem

With the wider ecosystem

The Data Strategy for Defence is part of a broader HMG agenda to leverage the power of data. This strategy has been developed to align with the wider data narrative of HMG (see Annex B) and international allies. Defence is part of a wider data ecosystem, where data interoperability is critical. This reinforces the need for a common approach within Defence to ensure that the whole of Defence remains connected and aligned to the wider ecosystem, see Figure 3.

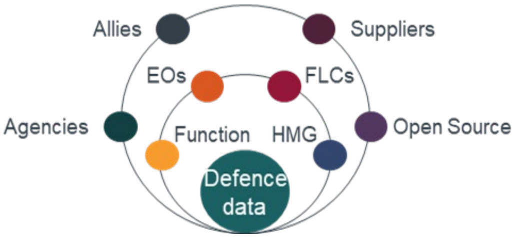


Figure 3 - The Defence Data Ecosystem

In line with the Defence Engagement Strategy, Defence will work increasingly closer with industry, vendors, suppliers and allies (i.e. FVEY, NATO) to develop data standards and best practices, increase access to open data sources, and assert common priorities by using existing and new initiatives, communities and forums.

The challenges and issues in using data within Defence and more broadly across government and allies can only be solved if organisations are agile, have strong partnerships and empower a culture of collaboration. A common narrative signals a drive to increase the pace in developing a digital government, reinforcing the importance for Defence to digitally transform and to use its data as a strategic asset.

> *'Defence will value data as a strategic asset, recognising it as the mineral ore that fuels integration and enables a system-of-systems approach.'*
>
> *Digital Strategy for Defence*

02 Ways

Defence will treat data differently

Across Defence, there will be a fundamental change in how it operates, data is everyone's responsibility and must be recognised and valued as a critical Defence asset. The ambition for battlespace advantage will only be realised through significant changes in behaviour and culture. To provide a better understanding of what this means for Defence personnel, this section below provides a set of example behaviours. Through the implementation of the strategy, roles will evolve with clear accountabilities in support of the Defence Data Lifecycle.

Senior Defence Leadership will:

- Appoint data leaders and setup data functions and governance within their organisations to drive the data agenda locally, in coherence with the Defence Data Office.
- Ensure that data is integral to key decision-making and operational activity, with enduring funding to govern, develop and maintain it locally.
- Recruit world-class and diverse talent with the data skills and capabilities to curate and exploit data locally, leveraging common data standards, automated interfaces and tools.
- Foster a cultural shift where data is front of mind for personnel, as opposed to an afterthought. Upskill and inspire their personnel on data skills and data professions.

Programme SRO's will:

- Demonstrate how data within the scope of their programmes will endure beyond the life of these programmes and continue to uphold the Data Rules.
- Adhere to Defence agreed data standards (e.g. Information Reference Architecture, APIs, classification, security and other NATO/industry standards (ISO)); and make a provision for good data management practices (e.g. stewardship, catalogue, classification).
- Treat data separate from any platforms, with its own set of mandatory data requirements captured within the key user requirements (KURs), providing clear understanding of how data will be exploited and for what purpose beyond the programme boundaries.

Capability Leads will:

- Ensure that data is integral to key decision-making around capability design and delivery, with enduring funding to govern, develop and maintain data.
- Adhere to Defence agreed data standards and good data management practices (e.g. stewardship, catalogue, classification).
- Ensure data is dynamic and can flow out of platforms for pan-Defence exploitation.

Functional Leadership will:

- Ensure that data is integral to key decision-making and operational activity, with enduring funding to develop and maintain it within their functional domains.
- Ensure that functional data within their domains live up to the Data Rules.
- Drive targeted interventions within their domains, in coherence with the Defence Data Plan (see Plan in Means section), to help Defence benefit from curated data, e.g. assertive management of suppliers and contracts, working with Defence Commercial Function to ensure Defence retains sovereignty over its data.

All Personnel (data and non-data professions) will:

- Uphold the Defence Data Rules by taking active roles as data stewards, data owners or by practicing good curation practices when manipulating data (e.g. data entry / data collection).
- Access and maintain Local and Enterprise Data Catalogues so data is accurate and available to all Defence personnel for exploitation.
- Complete mandatory data literacy training across Defence skills frameworks to develop a Defence-wide digital and data literate organisation.

Data Consumers will:

- Champion a 'smart' customer culture, taking accountability for defining clear requirements, seeking SQEP support at the right time, leading the use of common standards and templates, and ensuring compliance with data policies and procedures.
- Agree and prioritise Defence strategic digital needs to support a 'demand-led' data transformation approach. Data priorities are commonly agreed, enabling and supporting Defence in the fulfilment and delivery of its strategic agenda.

Defence Data Rules

The Defence Data Rules set out how Defence will treat data to become a connected enterprise, underpinned by an optimised business model for data exploitation, that ensures data is available and fit for analytics and analysis to drive better insights and outcomes. Adherence to the rules will enable Defence to leverage the investment on exploitation and innovation capabilities, such as the Digital Foundry and Defence Artificial Intelligence Centre (DAIC).

All programmes and activity will need to demonstrate compliance and will be assured against these rules. The lack of compliance around data must stop for Defence to avoid any future pain. Non-compliance to the Data Rules will result in Defence not realising data's strategic benefits and could be a blocker to obtaining programmatic approvals.

Defence Digital and the Defence Data Office will provide specialist services to support programmes and organisations pan-Defence in complying with the rules.

The six Data Rules Defence must apply:

1. Exercise *sovereignty* over data, including accountability and ownership
2. *Standardise* data across the Defence landscape
3. *Exploit* data at the most effective and relevant point in the value chain
4. *Secure digital* data at creation, curation, when handling, storing and transmitting
5. *Curate* data, ensuring it is assured, discoverable and interoperable
6. *Endure* data as an asset beyond individual projects

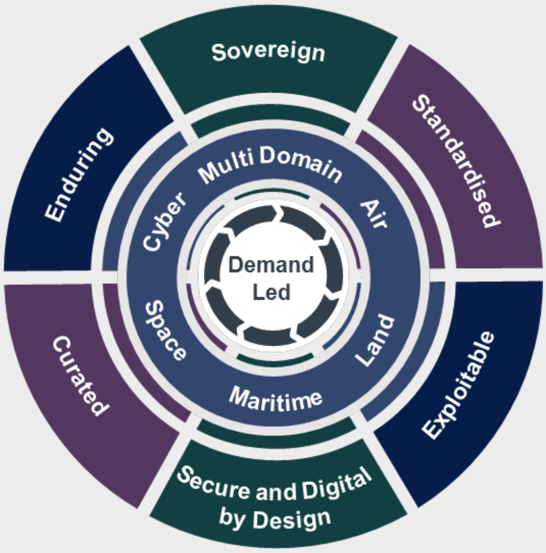
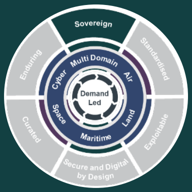


Figure 4 - The Defence Data Rules for all Defence to follow

The Defence Data Rules are not mutually exclusive

They are applicable to all within Defence to influence and advance our position within the wider data ecosystem

Establishing clear data guidelines for Defence personnel to adhere to



Sovereign

What does it mean...

Defence knows what data it has, where it is, how it is used, sets its policy and is able to assure its adherence to it, regardless of who has custody of it.

Defence must have sovereignty over its data to:

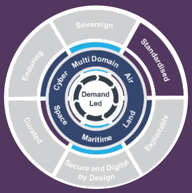
- **Unlock data held in the legacy estate** – Defence has a complex ‘brown-field site’ with thousands of legacy systems and associated data. Understanding this landscape is an imperative to its modernisation and the implementation of remediation efforts that facilitate its data integration and exploitation.
- **Break organisation, platform and technology silos** – To unleash the power of data, data cannot be trapped in silos, proprietary platforms or locked within Defence walls, unable to be accessed by other government partners and the wider data ecosystem when required.
- **Prevent commercial contracts locking data in** – A large amount of Defence data is held by suppliers and third parties, making it difficult to access, update without cost or leverage for exploitation. Defence needs to be a better customer, having greater control within contracts, ensuring that Industry protects Defence’s data and increases access to it.
- **Ensure there are governance mechanisms in place with clear data accountabilities and responsibilities for all** – There is a lack of understanding around what data Defence has and where it is, hindering Defence’s ability to access data, assure its quality and use and exploit it.

Defence will live up to the rule by:

- Taking accountability for building and managing Defence wide and local data capabilities.
- Making informed decisions when using external data or sharing data externally that may diminish Defence’s control.
- Adopting data management practices established in the Defence Data Management Strategy[1], with data owners and stewards accountable for understanding, maintaining and having control over their data. These accountabilities and responsibilities cannot and will no longer be outsourced.
- Following data controls and ensuring they are embedded in Defence governance mechanisms.
- Shifting culture and behaviours in a Defence enterprise that thinks of, manages and exploits data as an enduring valuable Defence asset, capable of enabling significant advantage.
- Complying with policies around curating, managing, governing and exploiting Defence data.
- Working with Defence Commercial Function to ensure data requirements are explicit in contracts with suppliers and third parties to enable frictionless availability of human and machine-ready data as needed.

> *We must take risks, nurture science and technological literacy, and* ***extract every drop of value from our data.”***
>
> *Professor Dame Angela McLean – Chief Scientific Advisor to the Ministry of Defence, Science and Technology Strategy 2020*

[1] Defence Data Management Strategy 2020



Standardised

What does it mean...

Defence follows industry, government, data management, and technical standards. The Defence Data Framework provides the artefacts and methods to be applied across Defence in a cohered manner.

> “*The **true value of data can only be fully realised when it is fit for purpose**, recorded in standardised formats on modern, future-proof systems and held in a condition that means it is findable, accessible, interoperable and reusable.*”
>
> *National Data Strategy 2020*

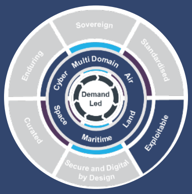
Defence’s data must be standardised to:

- **Enable reuse of data** – A lack of mastered sources of data across Defence leads to duplication of non-authoritative sources, multiple versions of the truth and sub-optimal use of limited resources.
- **Prevent perpetuation of data silos** – Limited coherence on the use of data standards neglects our opportunities to realise the benefits of interoperability, hindering data and capability reuse. This restricts pan-Defence exploitation practices and quality and reliability of our exploitation outcomes to serve as valuable information and intelligence.
- **Leverage a common technology architecture** – Disparate technologies perpetuate the complex Defence data landscape, preventing legacy systems and environments from being decommissioned and replaced by common enterprise-wide solutions.

Defence will live up to the rule by:

- Driving the delivery of Defence, government, industry and allies data standards (e.g. finance, commercial, geo-standards, ACP and FMN standards) and implementing appropriate governance controls for Defence to adopt data management practices and evidence adherence to standards for all capability delivery.
- Identifying and maintaining the true masters of data, reducing duplication and encourage re-use of existing data before creating new.
- Adhering to Defence Information Reference Architecture and Common Technology Architectures (CTA) for a modernised technology estate that supports legacy up-lift and obsolescence remediation activities.
- Supporting the Government-wide approach as set by the National Data Strategy[1] that ensures alignment on good practice and the standards needed to drive value and insights from data, enabling it to be used widely and effectively cross-government.
- Working with the Government's Data Standards Authority, contributing to identify and agree data mandated standards to adopt cross-government, and the enablers of international interoperability.
- Applying data assurance (see Annex E) to all programmes.
- Following and applying the Data Controls Framework to all capability development and programmatic delivery.
- Enabling access to Subject Matter Experts for all delivery.

[1] National Data Strategy – Updated 9 December 2020 - Mission three: Transforming government’s use of data to drive efficiency and improve public services



Exploitable

What does it mean...

Defence operates a frictionless business model that enables exploitation at the most effective and relevant point in the value chain (e.g. close to the customer through self-serve).

> *"We must become **data-centric and exploit** the data that we collect."*
>
> *General Sir Patrick Sanders, Commander Strategic Command*

Defence's data must be readily exploitable to:

- **Increase the value, opportunity and potential of our data** – The lack of control over our data is perpetuated via the barriers created by complex working models and business processes, inhibiting the exponential value that enterprise wide exploitation practices and capabilities can deliver.
- **Leverage across multiple sources** – Similar data requirements exist across the Defence Organisations in the pursuit of better insight and intelligence, but we are unable to integrate and therefore leverage federated data sources and skills for joint exploitation, leading to wasted effort through duplication and multiple versions of the truth.
- **Deliver at scale** – Technology within Defence is continuously advancing. This delivers large volumes of rich data that needs to be captured and processed to deliver operational advantage**.** Defence is not yet ready to scale up.
- **Ensure data skills are used for better analysis of data** – Data analyst resource and effort is wasted due to the need to source and prepare data before any actual analysis or analytics can be performed at the point of exploitation.

Defence will live up to the rule by:

- Recognising and treating data as a "need to share" asset, rather than a "need to know" requirement.
- Optimising Defence's business model for exploitation to enable quicker access to the right data and facilitate integration and interoperability across domains and wider PAG.
- Allowing data to interface, being available and machine-ready for consumption and exploitation regardless of where it is located through secure classification-based access.
- Driving a coherent and best practice use of advanced AI and analytics technologies that are common to its organisations and accessed remotely by all.
- Building and maturing a data professions framework that attracts, engages, develops and retains the talent for the Data Analyst and Data Scientist professions.
- Consuming API's, automated data interfaces and canonical models that are accessible and machine-readable.
- Ensuring data requirements and data sharing agreements are in place with suppliers and third parties to enable access to Defence and non-Defence data, supporting multi-classification data sharing and exploitation amongst all parties.

Secure and Digital by Design

What does it mean...

Defence Data is robust, fit for purpose, trusted and secure in a digital format. Data complies with legal, regulatory and ethical obligations.

Defence's data must be secure and digital by design to:

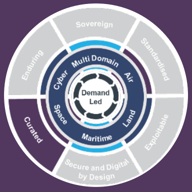
- **Contribute to the efforts to protect Defence networks and systems** – Defence faces ever present threats from malicious cyber activity; secure data supports in mitigating the risks and strengthening the rigorous cyber defence approach.
- **Control access to its own data** – Defence must ensure that secure and authoritative data sources are accessible by the right people for the right decisions to be made.
- **Enable resilient access to the data, with the means to detect when data is compromised and how it may have been affected** – Defence cannot risk nor compromise the data and information that it has access to. Data must remain secure at rest or in-transit with the right framework in place to guarantee its integrity, availability and confidentiality.
- **Comply with HMG, and Defence's legal, regulatory and ethical obligations over its data** – Data must be adequately curated to remain complaint and viable in a sustainable future, used within ethical principles and for the right purposes.

Defence will live up to the rule by:

- Ensuring data is securely created, securely curated, securely handled, securely stored and securely transmitted.
- Following the legal, regulatory and ethical guidelines in place to manage, exploit and dispose of data, such as the applicable Data Protection Legislation.
- Knowing where its data is and where it goes and ensuring data security roles and responsibilities are in place.
- Aligning with the Defence Data Management Strategy[1] for a common approach to the curation and maintenance of Defence data.
- Knowing the classification of its data, ensuring it is handled correctly and securely in line with privacy and confidentiality requirements.
- Applying the policies directed through the Defensive Cyber sub-strategy.
- Adhering to the Common Technology Architecture (CTA), underpinning the design of data receptacles and transfer mediums.
- Following and applying the Data Controls Framework to all capability development and programmatic delivery.
- Supporting the implementation of Identity and Access Management controls to ensure the right people access the right data and no more.

> *"As we drive increased use of data, **we must ensure it is used responsibly, in a way that is lawful, secure, fair and ethical, sustainable and accountable**, while supporting innovation and research."*
>
> *National Data Strategy 2020*

[1] Defence Data Management Strategy 2020



Curated

What does it mean...

Data is assured, discoverable, interoperable. It is separate from platforms and is always aligned to the Defence Data Framework and Standards.

> “*Competitive advantage will increasingly be gained from high quality, **well-curated and interoperable data,** seamlessly integrating our own data with data from outside Defence.*”
>
> *Science and Technology Strategy 2020*

Defence’s data must be curated to:

- **Break down silos** – Defence risks having large amounts of unusable and undiscoverable data across its Defence Organisations unless each organisation proactively manages its data and opens it up for the benefit of Defence’s wider use.
- **Leverage its own data** – Defence doesn’t have an enterprise understanding of where all of its data is, operating a large and complex environment of many systems and networks that cannot remain as black boxes. Defence needs an agile and scalable data architecture to support efficient and effective data supply to reduce duplication, increase reusability, and data discoverability.
- **Ensure decisions are based on trusted and quality assured data** – Defence needs data management and assurance practices that enable curated data to be relied upon, granting users and consumer access to curated, fused and exploitable data (to a single version of the truth). Operational and business decisions must be based on correct, timely and trusted data.

Defence will live up to the rule by:

- Organising, consolidating and cataloguing its data to enable visibility, consistency and re-use across organisations, as well as to allow multi-classification access (subject to security policies) to non-Defence consumers to drive national value.
- Adopting data management practices as directed by the Defence Data Management Strategy[1] for a common approach to the curation and maintenance of Defence data, ensuring data is trusted, robust and that its practices are enduring.
- Delivering on data accountabilities and taking pride by fulfilling their roles as data owners, data stewards and guardians of the Defence Data Rules.
- Driving the delivery of Defence-owned data standards, implementing appropriate governance controls for Defence to adopt data management practices and evidencing adherence to standards for all capability delivery.
- Embedding the data governance framework to advise, monitor and control data management practices.
- Contributing to the delivery of an enterprise data catalogue solution, a map of Defence data assets; and maintaining and using it to enrich Defence’s awareness, governance and understanding of its existing data assets.
- Applying data assurance (see Annex E) to all programmes.

[1] Defence Data Management Strategy 2020

Enduring

What does it mean...

Data is an enduring asset and capability. It persists beyond the life of a project and is continuously maintained to drive military and functional exploitation.

> *Data needs to be seen as* ***enduring.”***
>
> *Lt Gen Richard Wardlaw, Chief of Defence Logistics & Support*

Defence’s data must be enduring to:

- **Allow Defence to benefit routinely from data exploitation and new technology capabilities** – The value of data is progressively being acknowledged, but to realise its full potential, Defence needs to recognise that data requires dedicated and enduring effort and focus. Understanding and managing the asset must be second nature to all. When not treated as an enduring asset maintained throughout its life, data risks becoming a liability.
- **Ensure Defence consistently considers data's value and potential beyond its core project, programme, capability or operational need** – Defence can only realise the unlimited potential of data if it is always fit for purpose, available to its people and ready to be exploitable.
- **Build and mature a pan-Defence culture where data ownership is championed and those responsible are held to account** – Defence Organisations must not delegate ownership, they must be accountable for their own data – driving proactive behaviours to fix their own areas for the benefit of all.

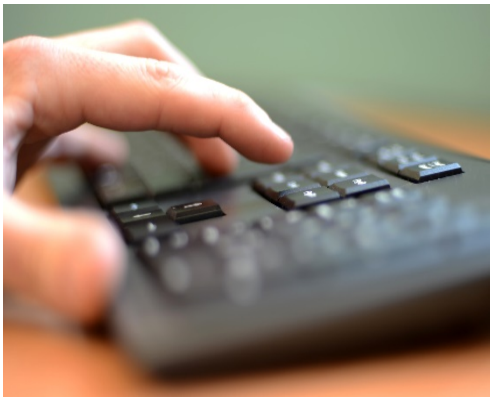
Defence will live up to the rule by:

- Championing the data theme; visibly raising the profile of data in Defence and endorsing the behavioural and cultural change that is needed to treat and manage data as a strategic asset and seeking constant experimentation and assessment of new data and analytical technologies.
- Cascading the Defence Data Rules, ensuring they are adhered to and are integrated in all programmes and digital investments.
- Embedding and adhering to governance, controls and standards.
- Holding themselves accountable for their data, acknowledging the value it has for the pan-Defence enterprise.
- Optimising Defence’s business model for exploitation to enable quicker access to data and facilitate interoperability across domains.
- Supporting the development of the DDaT Framework to upskill data professionals pan-Defence.
- Enabling data literacy and learning to enable programmes and personnel to think and embed data requirements and activities within their day-to-day responsibilities.
- Optimising Defence’s Operating Model (DOM) for multi-year planning, resourcing and funding for the development of common data capabilities pan-Defence.
- Delivering non-functional requirements (NFRs) to address the need for growth, maintenance and archiving of data.

Partnership and Collaboration

Partnership and collaboration is an underlying key theme across all horizontal layers of the Defence Data Framework. Both are necessary to further develop and build the framework and to accelerate the transformation of data across Defence

Defence Organisations:



The Data Strategy for Defence directs and coheres Functions, Commands and Enabling Organisations to drive and accelerate the data priorities across Defence.

The Defence Organisations are to take action to build and mature the Defence Data Framework, working together, leveraging the authority and cohering data with the Defence Data Office.

Each Defence Organisation will enable their data to power the Defence-wide Digital Agenda; and they will do so by asserting their presence as required and through the existing and emerging mechanisms to materialise the framework.

Defence Partners:

Defence data is rich and vast. It has enormous potential that can be further unlocked by working in partnership with government, allies, industry and oversight bodies. Data is a national asset. Defence has an obligation to enable the asset to be accessible to benefit and support the wider national agenda and the UK public. Defence, through the Defence Data Office, will actively engage and partner for excellence and advantage with its external stakeholders, seeking to drive innovation, lead strategic partnerships, harness data expertise, and enable more effective data exchange.

Defence will influence and cohere data across the landscape of stakeholders to accelerate the domestic and international agenda and build further upon capabilities for interoperability and cooperation. This will be achieved by:

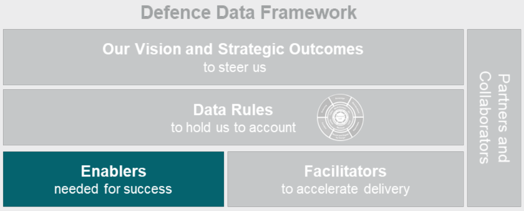
- Leveraging Defence’s commercial and supplier relationships to benefit from data (Defence and non-Defence data) access arrangements and innovation, with procurement reform being a strategic priority of CDDO. Increased sharing of data will also increase fusion with other data sources that will enable wider inferences, knowledge and intelligence.
- Enabling non-Defence consumers multi-classification access, use and analysis of Defence data (subject to security policies).
- Championing the adoption of best practice and development of controls and standards through membership within communities of practice, forums and external government and Industry committees.
- Cooperation with allies, Five Eyes, NATO and European counterparts, to ensure we can continue to work, operate and advance together.

03 Means

Enablers – Needed for Success

Within the Defence Data Framework, the Enablers are Organisation, People, Skills and Culture, Governance and Controls, Data Foundations and Exploitation. These are required to transform Defence into an enduring data driven enterprise. This allows Defence to coherently adapt to the fast-moving and complex data ecosystem that it is part of and for exploitation activity to deliver battlespace advantage.

The Enablers, in conjunction with the Facilitators, will enable the Data Rules to be adhered to and their benefits realised in an enduring manner.


Defence Data Framework

The Enablers

Organisation

Central leadership driving Defence's functional data mandate, with central and local teams working in lockstep to deliver the data vision.

People, Skills and Culture

Modernising Defence through adoption of a digital and data driven culture; investing in developing data professions and data-sawy personnel.

Governance and Controls

Embedding the governing structures and data controls that ensure decisions, investments and activities in Defence do not overlook data.

Data Foundations

Defence's priority driven standards, practices and policies to build and maintain robust data, preserving and enhancing its value.

Exploitation

Optimising data that is ready for exploitation through a common framework (processes, technology and tools), sustaining and evolving exploitation efforts in Defence.

The Defence Data Enablers → For Defence to deliver and serve

Enablers – Needed for Success

Organisation

What does the future data capability mean?

Defence will have central leadership driving Defence's functional data mandate, with central and local teams working in lockstep to deliver the data vision.

The current Defence business model is too complex for seamless exploitation and encourages the formation of silos, with ambiguity on requirements, the customer, data provider and where decisions are made. Simplification of the business model needs to be achieved before clarity and accountability can be realised in the data space. Building upon the Defence Operating Model and leading from within Defence Digital, data will be a horizontal capability connecting organisations pan-Defence, enabling collaboration with national and international partners on data.

Data is a Digital Functional Directorate within the Defence Digital Operating Model, and as one of its constructs, it will drive integration, cohesion and compliance for data. The function will work alongside the Digital Demand-capture function and the data leaders pan-Defence to prepare and respond to future demands. The Defence Digital Operating Model and data within, is further explained in Annex D.

The Director Chief Data Officer (CDO), as mandated by the Director General Chief Information Officer (CIO), leads the Defence Data Office and has a centrally led data mandate to ensure data is curated, interoperable and thus delivers effective and optimised data exploitation. Centrally specialised data services (see Annex D) will support Defence-wide organisations to cohere with the mandate.

What needs to be done?

All Defence personnel are accountable for Defence's data, with data capability and expertise developing and maturing across the enterprise, led and cohered by the central data function.

Defence Digital (Data Functional Directorate) Accountabilities

- Direct by asserting the Defence data mandate and authority on programmes, resources and governance.
- Provide the standards, frameworks and controls for Defence Organisations to use and align with when delivering locally.
- Govern by embedding data controls within the Defence governance mechanisms
- Assure by establishing and supporting technical governance frameworks and boards.
- Enable Defence exploitation by optimising the Defence business model and programmatic delivery approach towards frictionless exploitation.
- Enable a cultural shift through asserting the data mandate and defining and maturing data frameworks and data professions pathway to increase data skills pan-Defence.

Defence Organisations Accountabilities

- Deliver data outcomes locally, held to account through Defence agreed priority plan.
- Adhere to and align with the centrally defined and agreed standards, frameworks and controls, i.e., when procuring capability locally.
- Evidence the upholding of the Data Rules.
- Develop local expertise for exploitation and leverage the business model for exploitation.
- Maintain representation of local SQEP's to interact and partner with the Data Functional Directorate to deliver together towards fulfilling the vision for data.
- Allocate funding for development, governance and use of local data; enabling Defence-wide use and benefit for all.
- Driving forward resourcing across their functions with data skilled professionals.

Enablers – Needed for Success

People, Skills and Culture

What does the future data capability mean?

Defence must be modernised through the adoption of a digital and data driven culture that invests in developing data skills and data-savvy personnel. Defence will have expert data professionals, alongside all personnel being data-literate and data-aware. This will allow personnel to focus on what they were employed to do – make informed and effective decisions. Data literacy skills will be recognised as fundamental as weapon handling, with data as the lifeblood of operations and the firm base. Transforming the Defence culture and increasing data skills across Defence will allow management, control and exploitation of its data now and in the future.

What needs to be done?

Defence must enhance its data skills to drive efficient exploitation of data through innovative and advanced use of technology and tools.

- **Skills Frameworks:** Data needs to be recognised as a design principle within Defence's skills frameworks. This will ensure the need to transform data skills and ways of working is clear, and provides Defence with the means to deliver this data savvy workforce. The goal is to make data literacy a core skill. The wider Defence workforce will actively work with data, with data SQEP (data analysts/analysis function) leading on advanced and deep technical skills. Clear career and progression cycles, with learning pathways and rewards, will enable a sustainable and organic workforce model that has the right data mindset.

- **DDaT:** Defence will continue to further develop the DDaT framework for data professions, empowering world class data services that create enduring data capabilities within Defence across Commands, Enabling Organisations and Functions, and in support of government initiatives. As a strategic priority area of the CDDO, reducing the dependency on contractors and third parties by creating and improving in-house skills will create a sustainable and resilient workforce. These improvements in skills would also lead to higher productivity and reduced risk.

- **Diverse workforce:** Our people are our most important resource and innovation will only thrive if there is a diverse mix of skills, experiences, thoughts and approach. Recruiting, retraining and retention processes will be updated to inspire and attract local talent in an industry that commands a market premium. Diverse skills and experiences (spanning expert and literate) will improve how Defence uses and exploits data and are critical to operate in the information age.

- **Accountabilities:** The hub and spoke model will facilitate behavioural and culture change across Defence, with all personnel being clear on their accountabilities to create, curate and maintain endure data. All leaders across Defence will take accountability for their data, enforcing the Data Framework and sharing this with the wider Defence community. Leaders need to mandate their area's use of data, providing clear direction and incentives for better control of data, in benefit of transforming the culture across Commands, Enabling Organisations and Functions.

- **Communications:** Defence will be brought together within a cohered transformation journey that is clear in intent to embrace, invite and entice all personnel to be active participants and contributors to making Defence a data-led and data-savvy enterprise that endorses and lives up to the Data Rules.

Enablers – Needed for Success

Governance and Controls

What does the future data capability mean?

Defence must have governance and controls in place that ensure decisions, investments and activities do not overlook data, and focus on the right data priorities.

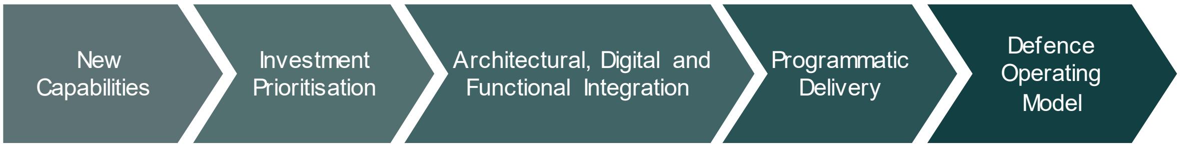
Defence, through the Defence Data Office, will assert the functional leadership for data, its assurance and critically, its exploitation pan-Defence. Partnering and cohering across Defence, the Defence Data Office will:

1. Lead the data mandate and assure through authority on data programmes, resources and governance. This will also include the assurance of spend, to ensure coherence in the employment of data capability, including analytic tools and technologies.
2. Collaborate with data owners and data SQEP to embed data controls and establish data capabilities, investments and activities authority in formal Defence governance mechanisms.

By leveraging its existing and new governance mechanisms, Defence will have appropriate data controls in place for all Defence key investment, capability and organisational decisions. Defence must also ensure, through defining clauses and data requirements in contracts, that industry self-regulates its management and use of Defence related data, protecting it and enabling it to be accessible for Defence to use.

What needs to be done?

The work to embed and mature Data within Defence governance mechanisms is in progress and comprises the embedding of data interventions across all decision-making points for:



New Capabilities

Investment Prioritisation

Architectural, Digital and Functional Integration

Programmatic Delivery

Defence Operating Model

The interventions provide the formal means to decide and govern the data decisions that Defence makes, as well as monitor the adherence to the data standards, policies and procedures that are created and enabled be these decisions. These can be described as (see Annex E for more detail):

- **Inserting Data into Defence governance mechanisms:** All existing DOM governance mechanisms will have data embedded. Data is inserted into existing JROC and IAC terms of reference and a senior Strategic Data Committee (SDC) has also been established as a 3* pan-Defence oversight forum and mechanism responsible for Defence's data outcomes, priorities and requirements. Other appropriate Defence mechanisms will be identified and relevant data measures incorporated (e.g. Refinement of the Information Defence Line of Development (DLOD)).
- **Bringing the management of Data under control:** Data will be managed using a common pan-Defence approach, with data hardwired in all future programmes and data relationships. TLBs and programmes will be able to demonstrate compliance with data rules (data fundamentals) and data standards.

Enablers – Needed for Success

Data Foundations

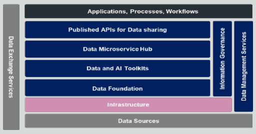
What does the future data capability mean?

Defence must adhere to and use priority driven Data Foundations (standards, practices and policies) to build and maintain robust data, preserving and enhancing its value and gaining pan-Defence synergies. Defence must move with the pace of the environment, therefore must not get too insistent on creating perfect data foundations that are detrimental to delivery. Defence must use what Data Foundations are available when and as needed.

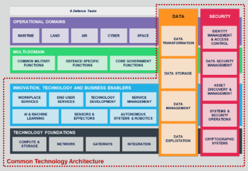
Data Foundational artefacts for Defence to adhere include:

- **Data Standards** – Rules around data, from data creation to archiving and deletion that Defence must follow when undertaking data activities.
- **Data Catalogue** – A map of data assets for users across Defence to find the data needed, associated policies and usage guidelines.
- **Information Reference Architecture** – Standards, design principles, patterns and technology recommendations for programmes to adhere and comply with.
- **Common Technology Architecture** – Framework detailing the common technical services that underpin the Digital Backbone. Data is one building block and encompasses the foundational services that support the exploitation of multi-classification data and its interoperability within and outside Defence boundaries. (see Annex F for more detail)
- **Establishment of data ownership and stewardship** – Methods for applying data ownership and stewardship for Defence critical data sets.

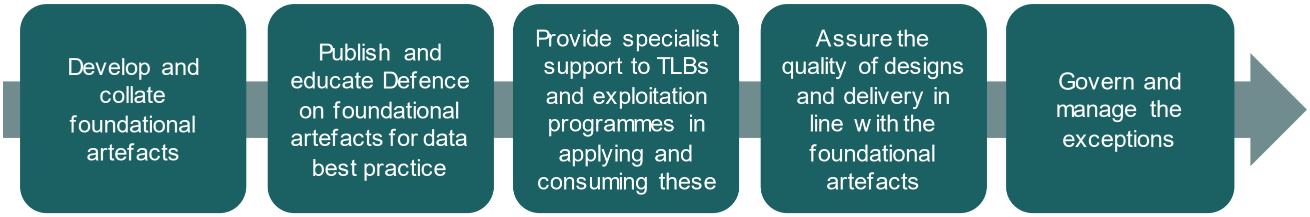
Information Reference Architecture



Common Technology Architecture



What needs to be done?



Develop and collate foundational artefacts	Publish and educate Defence on foundational artefacts for data best practice	Provide specialist support to TLBs and exploitation programmes in applying and consuming these	Assure the quality of designs and delivery in line with the foundational artefacts	Govern and manage the exceptions
Identify existing foundational artefacts for data available across Defence and those that need to be developed and collated.	Publish foundational artefacts and educate personnel on these through data working groups*, communities of practice, communication cadence and training academies.	Leverage the hub & spoke model so resources can be flexed in line with customer/programme demand and requirements.	Expert data resources support Defence programmes and transformations; providing assurance mechanisms for delivery in line with mandated foundational artefacts.	Insert data into Defence governance mechanisms to apply data controls on key investment, capability and organisational decisions.

*Data working groups will be set up as required - as part of business as usual, as a team within a data project workstream or to address data issues. They may be established at Defence level, covering Core Defence data or TLB level (Core and Non-Core Defence data).

Enablers – Needed for Success

Exploitation

What does the future data capability mean?

Data needs to be optimised for consistent, effective and where appropriate, collaborative exploitation across Defence Organisations. Currently, Defence's business model for exploitation is complex. This needs to be simplified to achieve a single version of truth, clarify roles and accountabilities and ensure Defence has a business model that is fit for exploitation.

This will be enabled by a common capabilities framework (processes, technology and tools), which in turn will deliver substantial benefit across Defence. Data of high quality is available and interoperable to personnel with the skills to analyse it and generate insights.

There are pockets of capability within Defence that are already delivering value through the effective exploitation of data, demonstrating the many opportunities Defence can benefit from.

An example: Project KRAKEN, a partnership between the Royal Navy and Industry, has accelerated the development of a fully integrated data platform. Bringing valuable and disparate data from numerous systems together on an enterprise wide scale, it has enabled all personnel to exploit previously unknown insight through new intuitive workflow and analytics tools. This has delivered significant operation and business value, including in the COVID-19 Response, Strategic Workforce Planning, Stores Contracting and Marine maintenance, and also encouraged behavioural changes across Defence around data.

See Annex H for more information and further examples of exploiting data to drive value for Defence

What needs to be done?

The Defence Data Office will support Defence Organisations with the adoption of common exploitation practices that operate within technical, legal and ethical frameworks. Common practices combined with optimised machine-ready data will enable organisations to interoperate effectively and realise the full benefit of Defence's investment in technology.

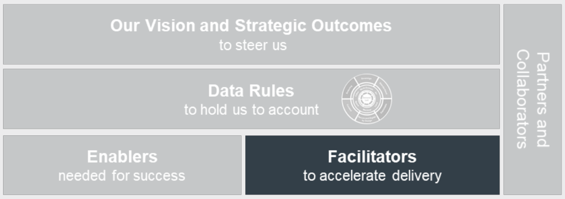
Adoption of common exploitation practices will be enabled by the following:

1. **A common data platform** to provide Defence Organisations with access to world class analytics, data science and artificial intelligence capabilities for the exploitation of data. Platform to be leveraged by exploitation initiatives such as Digital Foundry. *See Annex G for further information.*
2. **General adoption of modern solutions** such as cloud services, AI, robotics and emerging advanced analytics by Defence personnel across Defence Organisations to support decision making. Demand for the seamless exploitation of clean, available and interoperable data will grow exponentially as adoption of these solutions grows across Defence.
3. **Increased investment into the development of data skills** for all Defence personal, contributing to the levelling-up agenda by addressing skills gaps and bringing use of modern solutions to new areas of Defence.

Facilitators – Implementing the Strategy

The Facilitators, funding, plan and measures, are the supporting mechanisms required to co-ordinate and facilitate the execution of the strategy by establishing and embedding the Enablers needed for success.

Defence Data Framework



Our Vision and Strategic Outcomes
to steer us

Data Rules
to hold us to account

Enablers
needed for success

Facilitators
to accelerate delivery

Partners and Collaborators

Currently, there is a lack of understanding on Defence's data maturity benchmarks. Therefore, to deliver the Data Strategy, Defence will need to define those data benchmarks by which it can monitor progress and adapt accordingly. Regular tracking of milestones and progress made on agreed measures will provide trustworthy evidence of the data transformation taking place in Defence and the appropriateness of the targets set.

This strategy also provides a cohered funding approach for Defence to ensure there is enduring investment to deliver and sustain Defence's data assets and capabilities. In conjunction, the pan-Defence Data plan provided will mobilise and increase collaboration across the enterprise. It will be used to agree and prioritise a common agenda and local delivery plans. Only by all Defence personnel fulfilling their role within the data plan, will Defence be effectively transformed.

The Facilitators

Funding

Enduring funding approach required across Defence to sustain data assets and capability. All Defence Organisations and Programmes need to make explicit provision within their individual budgets to drive data activities in service of the Data Strategy for Defence.

Plan

Delivery plan with Defence milestones for all organisations to deliver, in order to achieve the data transformation agenda. These key milestones empower Defence to prioritise and coordinate investment and efforts towards their delivery.

Measures

Baseline measures, subject to Defence wide agreement, for all Defence to deliver on. Defence must track progress against these measures to ensure its transformation into a data driven enterprise and the effective delivery of the Data Strategy for Defence.

Facilitators – Implementing the Strategy

Funding

As a critical Defence asset, data requires dedicated, consistent and enduring funding and investment. This is similar to how any other critical Defence assets (e.g. our people, weapons) are funded so they can be maintained and utilised through life. Given the strategic importance of data, it is essential that the right amount of funds are invested at the right time, on the right data priorities across Defence.

In service of the data strategy for Defence, all Defence Organisations and Programmes need to make explicit provision within their individual budgets, to drive data activities, develop and curate exploitable data assets, and build the expertise across Defence to exploit these.

Defence Digital	TLB	Programmes
How will data activities be funded?		
Finite annual budget for the Defence Data Office, as part of the Digital Backbone budget within Defence Digital.	TLBs need to make explicit provision in their budgets, allocated to drive local data activities in coherence with the Defence Data Office.	Programmes need to make explicit provision in their budgets specifically for the delivery of data related components (incl. curation, management and development).
What will this funding enable?		
Direct, govern, assure compliance, and enable a cultural shift across Defence towards data exploitation. This will include: • Developing and rolling out the framework and processes • Assert control and govern data activities, investments and decisions	Support the development and adoption of the Defence Data Framework and drive local data activities including: • Staff local data leader and function • Assert local governance and interface with centre • Upskilling local personnel • Drive local data projects, e.g. catalogue	Design and deliver data components of Defence capability in clear alignment with the Framework including: • Deploying the right data skills • Adherence to the Data Rules • Compliance with foundational artefacts

Given the economic pressures and budgetary challenges, investment on data across Defence needs to be optimised. This can only be achieved if there is clarity and transparency on who is spending what money on data currently. The Defence Data Office will drive discussions with Organisations and Programmes to achieve transparency on current spend and cohere investment decisions going forward to ensure that investment decisions are appropriately prioritised and tied to strategic benefits.

Facilitators – Implementing the Strategy

Plan

The delivery plan ensures that Defence can cohere and integrate data across all domains, this is critical for the Digital Backbone and the MDI programme. The plan will allow Defence to work in synergy with partners across government, international allies and the intelligence agencies on the outcomes to be achieved and within the required timescales. This plan will inform and align with local data plans across Defence. The ambition is to co-ordinate the delivery of the enablers for success to accelerate value realisation from data exploitation across Defence.

Milestones aligned with Digital Strategy for Defence

	2021	2022	2023	2024	2025	Strategic Outcomes
Organisation	Defence Data Office operating at IOC	Establishment structures pan-Defence reflect data requirements	Defence Data Office operating at FOC	Maturing alignment with partners and industry to drive towards joint data outcomes (to include US DOD, NATO, FVEY, PAG, OGD's) Establishment structures pan-Defence at FOC		Data is curated, integrated and human and machine ready for exploitation Data is treated as the second most important asset only behind our People Our People are skilled and exploiting data to drive advantage Defence are data leaders with partners, allies and industry
People, Skills and Culture	Data professions framework updated for all Defence Data roles (Incl. DDaT and other relevant frameworks) providing clear career progression paths	Critical Data office posts delivered, significantly increasing Defence Digital capability	Data skills framework adopted; L&D paths established and funded with clear career progression established	Defence workforce is transformed, with the right mix of data skills (highly skilled, data-literate, data-aware) and diverse, motivated and flexible people		
Governance and Controls	Delivered cohered technical expertise, assurance and capability that integrates to a common set of skills, rules and standards	Chain of command established and embedded for data decision making across Defence governance Data Controls Framework embedded in programme assurance	Capability and programme delivery compliant with Data Controls Framework driving benefits (incl. reduced costs, faster delivery, reduced risk)			
Data Foundations	Defence Data Framework delivered, enabling interoperable data and common exploitation Data Fundamentals delivered, driving standardisation, interoperability and consumption	Information Reference Architecture established to drive architectural standardisation across Defence. Then matured in response to priorities set by data governance forums Data controls fully adopted in TLBs and Programmes	MOD curated data mapped for 3 lines of business			
Exploitation	Common data exploitation platform and approach at MVP (human and machine) enabling initial use by Foundry	Data Estate Map enabling data users and consumers to access the data they need (IOC)	Data Estate Map enabling pan-Defence users and consumers to access the data they need (FOC) Initial data exploitation capability at IOC	Mature data exploitation capability at FOC		

Facilitators – Implementing the Strategy

Measuring Success

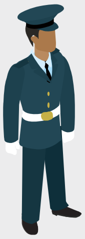
The following measures provided for each of the Enablers for success are example measures. These need to be defined and agreed across Defence as a whole. Upon agreement, Defence Organisations must align and be accountable for their own measures according to their size, function and the complexity of their specific organisation.

Enabler	What does success look like?	How will we start measuring success? (examples – to be fully defined)
Organisation	Defence has an operational hub and spoke model with central leadership from the Defence Data Office driving Defence's functional data mandate. Defence Organisations have structured local data functions to deliver the Defence data vision. Accountabilities across the hub and spoke are understood, hard-wired relationships are established and Defence's data priorities are continuously reviewed, agreed and acted upon.	• Defence Operating Model formally recognises the hub and spoke model for data across Defence • All Defence Organisations have local data leadership and teams in place who drive and champion the Defence data agenda locally by 2025
People, Skills and Culture	Defence has an inclusive and diverse workforce. Data learning opportunities are accessible to all employees, from "basic literacy/awareness" to "expert professionals" skills through Defence's skills frameworks. Data professionals have clear career progression pathways. Culture and behaviours are continuously shifting across Defence, with data activities and requirements considered early on in programme, capability and investment planning. Data is second nature to day to day operations for Defence personnel.	• 60% increase in data SQEP across Defence • Personnel surveys suggest that more than 80% of data professionals are pursuing data progression pathways • All Defence data professionals have access to the DDaT framework • All Defence personnel have completed their data-literacy training and are able to pursue data up-skilling opportunities and careers
Governance and Controls	Defence has data fully inserted and operational in key governance mechanisms, with data controls applied across all capability and programme delivery frameworks. Data is no longer an after-thought when it comes to capability investment decisions and is integral to all strategic decision-making. Defence data dedicated governance bodies and their local equivalent structures are widely established, operating coherently with the Defence Data Office.	• All SROs are able to demonstrate data KURs for all capability development within the Information DLOD are clearly defined, budgeted for and delivered upon • All new signed contracts address issues around data sovereignty resulting in the balance of benefit in favour of Defence Organisations • Data ownership and stewardship for all Defence data domain have been established and is operational through Defence personnel
Data Foundations	Defence knows what data it has and where it is. Data standards across Defence, OGD partners and industry are commonly and coherently applied. Duplication incidents are continuously prevented along with a legacy data estate that is replaced through the adoption of Defence's Information Reference Architecture and Common Technology Architecture.	• Target TLBs using existing government Data Maturity level (between 1-5). Expectations of observing at least an increase in maturity level of 2 points • Defence Data Catalogue is fully operational with adoption and integration across all organisations • 80% Defence Organisations have adopted the data technologies as defined in the CTA
Exploitation	Defence is following a common pan-Defence exploitation framework, and is exploiting data according to relevant ethical, regulatory, security and legal frameworks. Self-service solutions are encouraging and enabling non-data customers to exploit data through intuitive interfaces. Data professionals are able to introduce and test new technology for fast adoption and integration; enabling cutting edge solutions to be leveraged.	• All Defence Organisations are leveraging the common data and AI frameworks and common data platforms. This results in timely, cost-effective and simpler exploitation of data for the same outcomes • 70% increase in customer satisfaction when using self-service solutions to exploit their data

Annex

Annex A: What we mean by Data

As stated in the National Data Strategy, “Data is notoriously hard to define – and it means different things to different people”. The exact definition of ‘data’ can be ambiguous across Defence, but this strategy defines data as records, facts or numbers across the value chain, from collection and storage through to exploitation, and its role in decision-making. In a Defence context, examples of what data is and where it is used include:



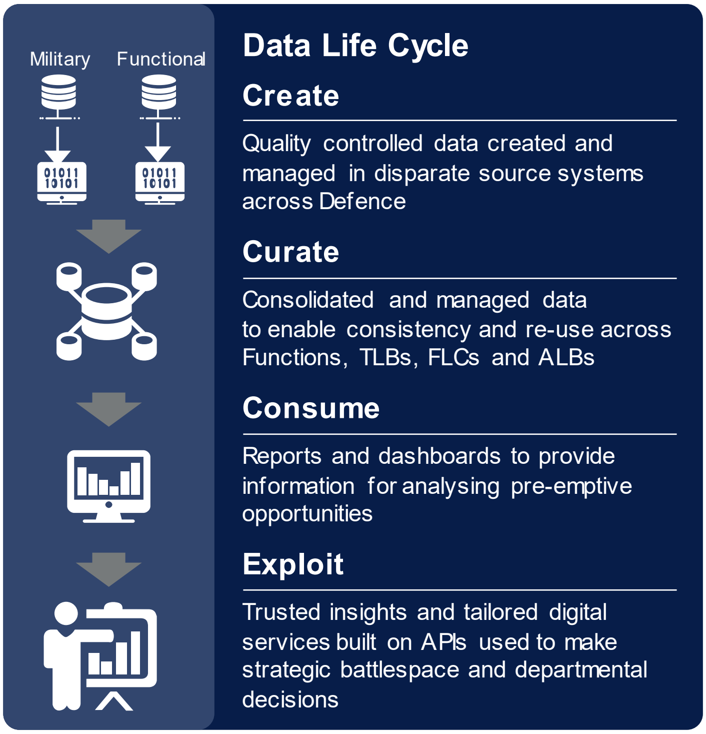
The Royal Air Force needs to be able to accurately monitor fuel consumption across units, groups and platforms in order to contribute to the UK’s 2035 target of reducing national carbon emissions by 78%.

Planning teams need access to up-to-date people, skills, training, certifications and availability data to staff critical projects and overseas deployments.

Platform information needs to be analysed to optimise serviceability, range and use. This further informs balance of investment, force development and planning decisions.

When data is put into the relevant context, it becomes information, which in turn, can be considered or become data into other decision-making processes. Data combined with the human (or machine) factor of analysis, treatment and/or assessment leads to intelligence to inform decisions. Further detail on information in Defence can be found in the Defence Information Strategy (document in production).

Data can be about people, things or systems. Data about people can include personal data, such as contact details, certifications, deployment records. Personal data must be processed in accordance with all applicable data protection laws and relevant privacy and security policies, its usage cannot be exploited freely. Platform data can include mission summaries, navigation records and sightings. Data is also increasingly used to describe location, such as geospatial reference details. Logistics planning are hugely reliant on assets and spares inventories to decide optimal routing to areas of need.



Data Life Cycle

Create

Quality controlled data created and managed in disparate source systems across Defence

Curate

Consolidated and managed data to enable consistency and re-use across Functions, TLBs, FLCs and ALBs

Consume

Reports and dashboards to provide information for analysing pre-emptive opportunities

Exploit

Trusted insights and tailored digital services built on APIs used to make strategic battlespace and departmental decisions

Figure 5 – The Data Lifecycle

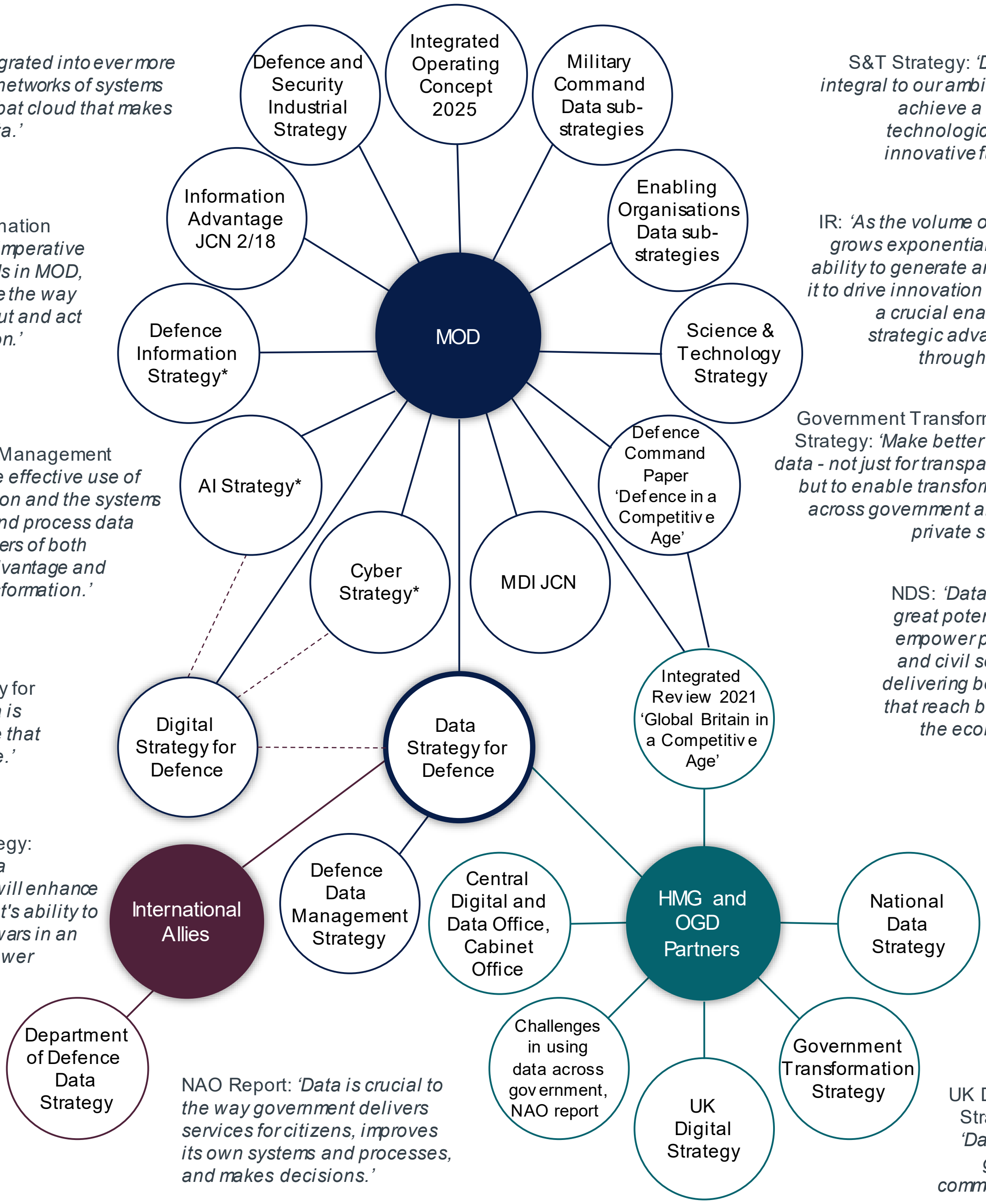
Data in Defence can be categorised in terms of Core Defence Data or Non-Core Defence Data. Additional information on the methods of data categorisation is provided in the Defence Data Management Strategy 2020.

The Data Strategy for Defence seeks to define, embed and implement a data framework for Defence; through which the management and governing structures along with the technology and functional enablers, will provide Defence with the standards, procedures and policies to manage its data life cycle.

From data creation at entry points through to analytics, exploitation and disposal; data flowing through Defence’s digital backbone, will be known, curated and machine-ready in benefit of Defence’s innovation agenda for advanced exploitation.

Annex B: Defence Data in a Wider Context

The Data Strategy for Defence is part of a broader HMG agenda to leverage the power of data. Figure 6 shows a selection of strategies and policies that have driven the development of this strategy. The strategies and policies used in our research do not represent an exhaustive list but do present, see quotes extracted across the strategies and policies, the important role of data in the future.


MOD
Defence and Security Industrial Strategy
Integrated Operating Concept 2025
Military Command Data sub-strategies
Information Advantage JCN 2/18
Enabling Organisations Data sub-strategies
Defence Information Strategy*
Science & Technology Strategy
AI Strategy*
Defence Command Paper 'Defence in a Competitive Age'
Cyber Strategy*
MDI JCN
Integrated Review 2021 'Global Britain in a Competitive Age'
Digital Strategy for Defence
Data Strategy for Defence
International Allies
Defence Data Management Strategy
Central Digital and Data Office, Cabinet Office
HMG and OGD Partners
National Data Strategy
Department of Defence Data Strategy
Challenges in using data across government, NAO report
UK Digital Strategy
Government Transformation Strategy

IOPC: '*Be integrated into ever more sophisticated networks of systems through a combat cloud that makes best use of data.*'

Defence Information Strategy: '*It is imperative that at all levels in MOD, people change the way they think about and act with information.*'

Defence Data Management Strategy: '*More effective use of data, information and the systems that manage and process data are vital enablers of both operational advantage and business transformation.*'

Digital Strategy for Defence: '*Data is the mineral ore that drives Defence.*'

US DOD Strategy: '*Improving data management will enhance the Department's ability to fight and win wars in an era of great power competition.*'

NAO Report: '*Data is crucial to the way government delivers services for citizens, improves its own systems and processes, and makes decisions.*'

S&T Strategy: '*Data is integral to our ambition to achieve a highly technological and innovative future.*'

IR: '*As the volume of data grows exponentially, the ability to generate and use it to drive innovation will be a crucial enabler of strategic advantage through S&T.*'

Government Transformation Strategy: '*Make better use of data - not just for transparency, but to enable transformation across government and the private sector.*'

NDS: '*Data holds great potential to empower people and civil society, delivering benefits that reach beyond the economy.*'

UK Digital Strategy: '*Data is a global commodity.*'

Figure 6 – A selection of the International, UK and Defence strategies and policies to which the Defence Data Strategy for Defence relates.

* Document in production

Annex C: Last Mile Logistics Challenge

Introduction

The aim of this vignette is to demonstrate the potential use of autonomous systems to deliver mission-critical supplies, focusing on the challenging 'last mile' logistics problem in the land environment. The 'last mile' logistical resupply predominantly involves the delivery of combat supplies from the forward-most logistical resupply location in the Area of Operations (AOR), (such as a physical base or a logistics/infantry vehicle) to personnel engaged in combat operations.

Although relatively small in distance, these resupply activities are challenging as they are in an environment that is typically hostile, complex and contested. These activities need to deliver vital supplies quickly and efficiently in order to maintain operational tempo and enable successful mission outcomes. It's important to note the last mile is a concept, not a fixed distance.

Background

Currently, the British Army resupplies the frontline using a variety of ground based and aerial delivery platforms depending on the circumstances and the nature of operation taking place. They can vary from transport aircraft and helicopters, large trucks to quad bikes with trailers or soldiers on foot.

The resupply forward users will vary in size, location and requirements, however typical examples include a light force operation with dismounted soldiers on-foot or a mechanised operation using armoured vehicles. They both operate in hostile, tactically constrained forward-most locations of the battlespace.

Aim

- Reduce the demand on existing platforms and infrastructure
- Reduce the risk and reliance on military personnel during last mile resupply
- Increase the efficiency of the last mile logistic resupply operations with agility, pace and accuracy
- Provide an assured resupply capability for forward military users to enable more agile operations in complex environments

Scenario

A light force operation with dismounted soldiers on-foot requires many logistical elements that will require consistent resupply during a mission. Two of these elements would be radio batteries and rations. The sensor component for each of these elements will be different as described and could be manual or automated.

In a fully automated scenario, the radio batteries will self-report via the integrated C2 system This initiates automated logistical re-resupply as part of the J4 Standard Operating Procedures (SOPs). The Commander is also informed. In a more manual scenario such as delivery of rations, a report or request would be sent via the C2 system requesting ration replenishment at a specific time and location.

The decision to act on the request and send the replacement batteries is fully automated. Only if there are impelling operational circumstances would the Commander need to be involved in the decision, for example if battery supplies were low and real time priority calls needed to be made.

The effectors could be an unmanned air asset delivering to an unmanned ground system. A Mission Management & Asset Planning capability could perform vehicle allocation and mission planning or an Unmanned Asset Command and Control (C2) and ground control system can perform autonomous vehicle routing such as terrain analysis, re-routing, vehicle communications and dynamic re-tasking.

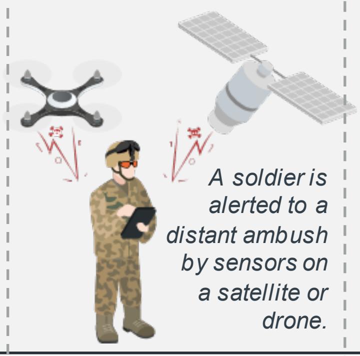
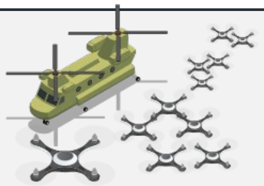
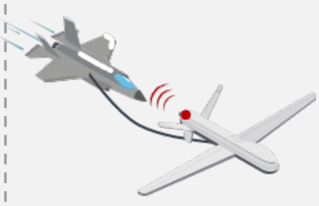
Benefits with autonomous last mile resupply include:

- **Effort.** Traditional resupply consumes substantial assets, time and manpower and can be dangerous in hostile locations.
- **Execution.** Resupply can also affect the tempo of an operation and the availability of personnel resulting, in a delay to operations
- **Combat Effectiveness.** Troops often need to carry additional supplies to reduce resupply uncertainty, which could result in significant physical burden, an increase in the risk of injury and reduce combat effectiveness.

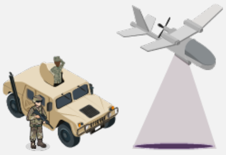
Annex C continued: Additional Scenarios (Part 1)

As presented on page 4, fully unleashing the power of Defence's data, connecting sensors, decision makers and effectors, will deliver impact that saves lives, resources and time. The below scenarios are further examples of the role data can play across Departmental activities:

- Fight: Protecting people, territories, values and interests at home and overseas.
- Operate: Key operations to keep MOD running and to meet core objectives.
- Intelligence: Wider collaboration outside of MOD, with government, allies, industry and oversight bodies.

	Sensors detect a physical or digital signal	**Decision makers** decide on the best course of action	**Effectors** respond to signals as per the decision
Fight			
Soldier in hostile territory	 *A soldier is alerted to a distant ambush by sensors on a satellite or drone.*	*Artificial Intelligence devises a number of optimal responses and best option is selected by soldier.*	 *There may be an air strike summoned, a swarm attack by drones ordered, or the enemy is paralysed with cyber weapons.*
Fast jet requires fuel	*Fast jet triggers low fuel alert.*	*Fast jet automated request sent for aerial refuelling to carrier base drones.*	 *Drone delivers fuel to fast jet.*
Smart pill for medical emergency	*A smart pill is swallowed by an injured soldier to detect extent of injury.*	*Information from pill is sent to paramedic or surgeon located remotely to decide on treatment.*	*Using virtual reality, fellow personnel on front line is guided by paramedic or surgeon in undertaking treatment.*

Annex C continued: Additional Scenarios (Part 2)

	Sensors detect a physical or digital signal	**Decision makers** decide on the best course of action	**Effectors** respond to signals as per the decision
Operate			
Malware threat	*A sensor detects a cyber threat in the network.* 	 *Data is fed from the sensor to the system to decide course of action or to the cyber team to act.*	*A patch secures the system.*
Personnel fitness	*A fitbit tracks the fitness of personnel.* 	 *Data on personnel fitness is transmitted to deployment centre to take decision on mission readiness of personnel.*	*Personnel are deployed for action or the personnel receives an updated fitness plan.*
Intelligence			
Anti-Poaching	 *Satellite images detects potential poaching in a protected wildlife reserve.*	*Transmitted to anti-poach local authorities and teams, with proximity data and size of threat. Military support agreed.* 	 *Military personnel deployed, supported by surveillance drones in aid of host nation to protect wildlife or arrest criminals.*

Annex D: Digital Operating Model (with Data perspective)

The Digital Operating Model provides a strong, connected and cohesive functional team working as a single entity across the federated Defence landscape. Figure 7, extracted from the Digital Strategy for Defence, presents all four constructs: Digital Function Directorate, Demand-capture from commissioning, Defence CIOs (and the equivalent Data leaders working alongside the Director CDO) and Service Delivery. Data resides within the Digital Function Directorates alongside Strategy, Digital Enablement, Cyber Defence and Risk and Functional Integration; driving integration, cohesion and compliance.

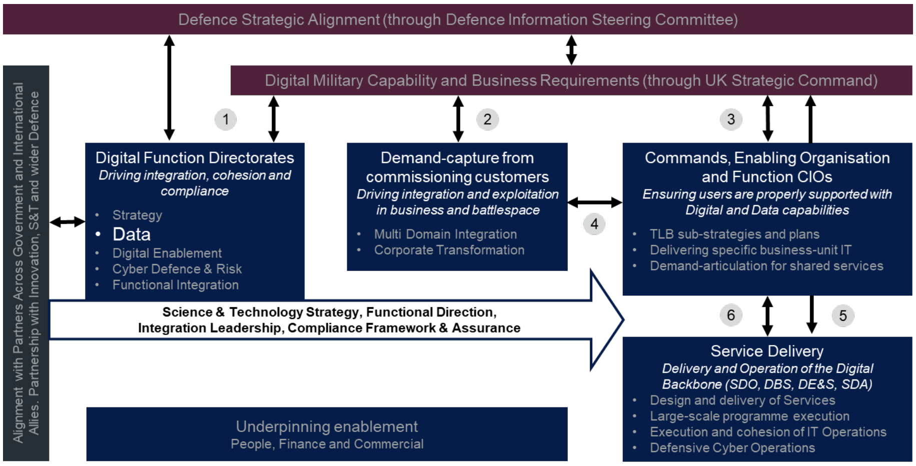

Defence Strategic Alignment (through Defence Information Steering Committee)
Digital Military Capability and Business Requirements (through UK Strategic Command)
Alignment with Partners Across Government and International Allies. Partnership with Innovation, S&T and wider Defence
1
2
3
Digital Function Directorates
Driving integration, cohesion and compliance
• Strategy
• Data
• Digital Enablement
• Cyber Defence & Risk
• Functional Integration
Demand-capture from commissioning customers
Driving integration and exploitation in business and battlespace
• Multi Domain Integration
• Corporate Transformation
4
Commands, Enabling Organisation and Function CIOs
Ensuring users are properly supported with Digital and Data capabilities
• TLB sub-strategies and plans
• Delivering specific business-unit IT
• Demand-articulation for shared services
Science & Technology Strategy, Functional Direction, Integration Leadership, Compliance Framework & Assurance
6
5
Service Delivery
Delivery and Operation of the Digital Backbone (SDO, DBS, DE&S, SDA)
• Design and delivery of Services
• Large-scale programme execution
• Execution and cohesion of IT Operations
• Defensive Cyber Operations
Underpinning enablement
People, Finance and Commercial

Figure 7 – Digital Operating Model constructs and linking processes

Linking Processes and Procedures *(including Data perspective for indicative data services)*

1 **Defence Strategy alignment.** Defence Information Steering Committee (DISC) oversight to ensure deployment and use of relevant, leading-edge digital capability. Work with UK StratCom to inform investment and prioritisation in integrated capabilities. **Data:** *The Strategic Data Committee (SDC) reports to DISC leading the Data agenda.*

2 **Multi Domain Integration (MDI) and Corporate Transformation alignment.** Enabling the objectives of the other horizontal Transformation programmes. Leadership into the MDI Change Programme to improve strategic enablement in key programmes, and through 'Moonshots'. **Data:** *Enabling Data priorities to be led by business demand.*

3 **Specific TLB/ALB and Function IT alignment.** Functional leadership into accelerated strategic enablement and alignment. CIOs drive coherence and cohesion within the overall Function strategy. **Data:** *Data and Digital leaders cohering on Data priorities.*

4 **Co-ordination and scaling-up of exploitation.** Working in partnership with Head Office, TLBs, Functions to accelerate the secure adoption and exploitation of data-driven, software-defined capabilities across Defence. **Data:** *Data and Digital leaders cohering on Data capability delivery with the support of centrally provided data services (Figure 8).*

5 **Requirements setting and Capability sponsorship for specific programmes.** Capability Sponsors lead the exploration against requirements, with Defence Digital assuring the alignment with Digital Strategy. Commands' Capability Directors sponsor capability requirements through all phases. **Data:** *Data requirements and assurance practices are embedded in all digital delivery.*

6 **Service Demand Management and Cyber Incident Management.** End-to-end IT Operations Service Management, setting the 'Rules of the Road'. Management of Defensive Cyber Operations (DCO) and incidents through Defence's federated Cyber Security Operating Capability (CSOC). **Data:** *Data design is compliant with data standards.*

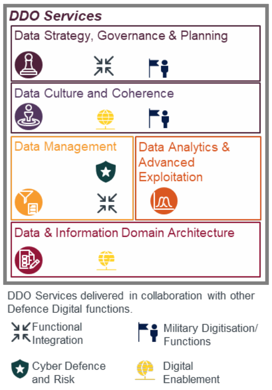
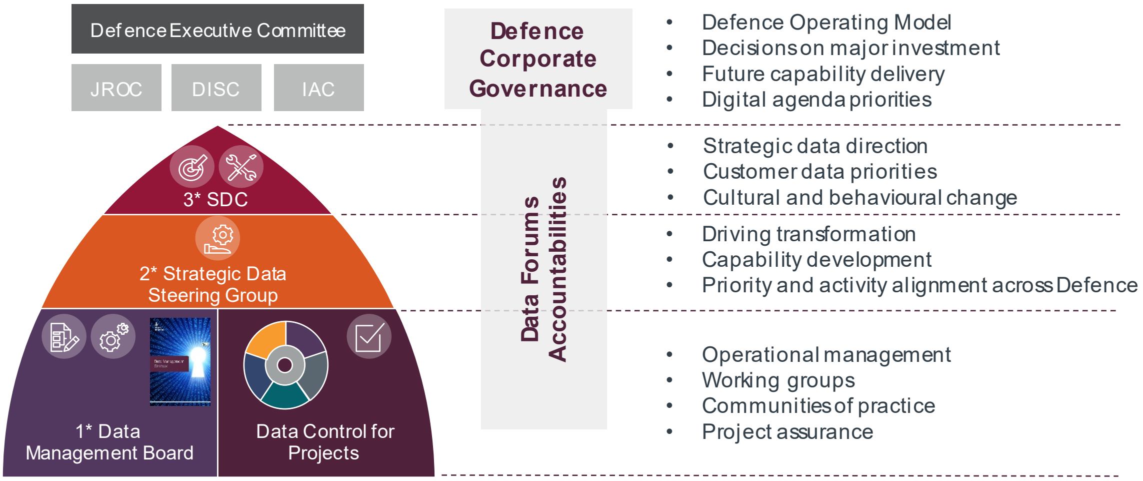

DDO Services
Data Strategy, Governance & Planning
Data Culture and Coherence
Data Management
Data Analytics & Advanced Exploitation
Data & Information Domain Architecture
DDO Services delivered in collaboration with other Defence Digital functions.
Functional Integration
Military Digitisation/ Functions
Cyber Defence and Risk
Digital Enablement

Figure 8 – Defence Data Office Services

Annex E: Governance and Controls - Inserting data into Defence Governance Mechanisms

Progress has been made in formalising data into governance mechanisms across Defence. Figure 9 shows how the data functional leadership mandate is represented on various 3* and 4* boards through direct and indirect attendance of the Defence CDO. The data mandate has also been inserted into existing JROC and IAC terms of reference.

A senior Strategic Data Committee (SDC) has also been established to provide data with a dedicated supporting pillar and is the 3* pan-Defence oversight forum and mechanism responsible for Defence's data outcomes, priorities and requirements. In addition, in order to manage the complexities of data in a large organisation like Defence - that operates under a hub and spoke model - a hybrid model of data governance has been designed.



Defence Executive Committee
JROC
DISC
IAC
3* SDC
2* Strategic Data Steering Group
1* Data Management Board
Data Control for Projects
Defence Corporate Governance
Data Forums Accountabilities

- Defence Operating Model
- Decisions on major investment
- Future capability delivery
- Digital agenda priorities

- Strategic data direction
- Customer data priorities
- Cultural and behavioural change

- Driving transformation
- Capability development
- Priority and activity alignment across Defence

- Operational management
- Working groups
- Communities of practice
- Project assurance

2* Strategic Data Steering Group

- Owns Data Strategy for Defence and assure coherence across all local data strategies.
- Defines Defence Data Priorities and Roadmap; confirming the key Capability delivery programmes where efforts and resources will be focused.

1* Data Management Board

- Drives the adoption and implementation of the Data Management Framework, identifying Data Owners and Stewards across the organisations to improve curation practices and quality of the data.
- Delivers data foundational priorities through the establishment of working groups.

Figure 9 – A view of the Defence Corporate Governance mechanisms where data has been inserted and established Data Forums.

Annex E continued: Governance and Controls - Bringing Management of Data under Control

Alongside inserting data into Defence's governance mechanisms, there has been progress in bringing management of data under control through standardising data management and delivering data assurance.

Standardising the Operational Management of Data

The Defence Data Office provides the Data Framework to bring consistency and coherence to the management of data pan-Defence, and mandate adherence to it.

Foundational capabilities are being developed to bring operational management of Defence data under control. These will bring consistent frameworks and methods to manage Defence data assets in a manner that enables quality, interoperability and drives value. The 1* DMB brings Defence data practitioners, working groups (pan-Defence data SQEPs) and communities of practice together, to own, develop, maintain, and mature their data domains under a common framework.

Implementing and Delivering Data Assurance

Programmatic and transformational delivery will adopt and apply mandated data standards.

Expert resources will be available to delivery teams to ensure data standards and data policies are coherently used and enable the production of data and technically compliant designs and solutions that progress into delivery.

Delivery teams will fund access to this expert advice through available and future resource frameworks (e.g. DIPS), as advised by the Defence Data Office. This will also be aligned to the Functional Integration governance model for coherence (middle pillar in Figure 10), where data actively participates and contributes.

All digital delivery will be subject to data assurance through these existing mechanisms within the Functional Integration in Defence Digital (middle pillar in Figure 10). This will enable the implementation of a coherent assurance process that enhances and builds upon other Coherence Lateral Boards across Defence Digital (right pillar in Figure 10).

Data assurance, as part of technical assurance, could in some instances be franchised to more mature organisations in Defence. This could also mean oversight accountability through the Defence Data Office within the Functional Integration agreed framework.

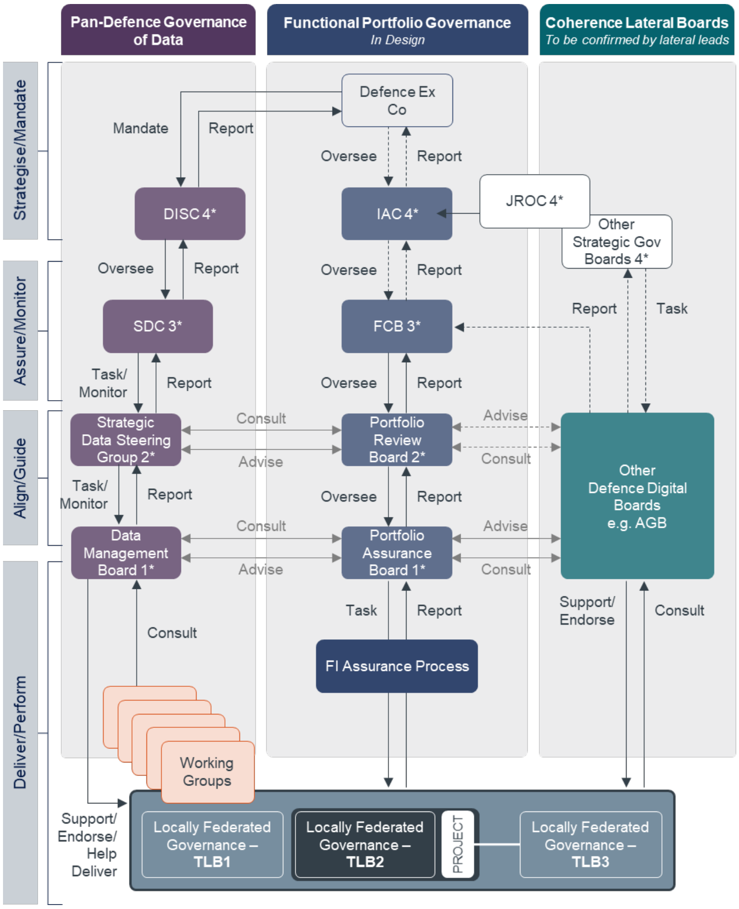


Figure 10 – A view of data assurance and data boards as part of the wider governance and assurance mechanisms across Defence.

Annex F: Common Technology Architecture*

Purpose

The Common Technology Architecture (CTA) is a framework and architectural approach under which the detailed technical definition of the Digital Backbone and its underlying components and services can be developed. It will also serve as the framework of policies, standards and reference patterns against which the delivery and adoption of the Digital Backbone can be guided and governed.

Drivers for Change

- ✓ the need to enable our mobile first workforce
- ✓ to collaborate and interoperate both internally and externally
- ✓ to take advantage of the enhanced maturity and accessibility of cloud and edge computing
- ✓ to respond to the rapidly evolving cyber threat
- ✓ to enable multi-domain working, and
- ✓ to better nurture our ability to exploit new and emerging technologies.

Delivery of the CTA and its underpinning artefacts will enable Defence to rapidly deliver new technology by providing the architectural building blocks from which delivery projects and programmes can connect to and make use of the Digital Backbone.

The policies and standards that will underpin the CTA will also set the rules to be followed (internally and by external partners) to ensure coherence across the technology estate and enable Defence to fully realise its vision for seamless data sharing, integration and interoperability.

Targeted Outcomes

There are several specific technology outcomes being targeted through the CTA. These further strengthen the role of the CTA in supporting the Data Vision for Defence.

Increased Technology Integration & Interoperability

Integration on all fronts across Defence and its military domains, across government and with external partners (e.g. allies - NATO, suppliers, etc) is vital for continued security and prosperity. Defence systems will need to be purposefully (re)designed to ensure data can be easily shared and exploited and substantially increased levels of data and systems integration are achieved.

Modernised Technology Estate

The CTA will enable delivery by driving and cohering the delivery of modern, shared services; defining and guiding Defence towards the target state for modernised pan-Defence technology and providing a framework to guide legacy up-lift and obsolescence remediation activities.

Multi-Classification & Multi-Cloud Hosting Environment

One of the foundational building blocks of the Digital Backbone is the delivery of a multi-classification, multi-cloud and hyperscale Cloud environment. This supports increased data sharing and exploitation across security classifications, mobile access to Defence systems and rapid development and scaling of applications to meet increasing demands and possibilities.

Secure & Resilient Next Generation Network

The development of a secure, resilient and modern network is integral to delivering and enabling full exploitation of the Digital Backbone. This will support the seamless access to, and exploitation of, data, regardless of location. This will in turn enable the game changing and innovative use cases envisioned in the Digital Strategy and the Integrated Review, for example, real-time use of Artificial Intelligence on the battlefield.

Defining a Common Technology Architecture

The CTA is composed of a number of hierarchical building blocks, expressed as technology services (see Figure 11).

Level 1 (Conceptual). Broad outline of how technology services are categorised at the highest level, e.g. Data

Level 2 (Logical Service Categories). Breakdown of the conceptual architecture into categories of technologies, e.g. Data Management

Level 3 (Technology Services). Granular technology services used as individual building blocks to deliver architectures and solutions.

Data: Foundational services that support the exploitation of data as a strategic asset (Data Transformation, Data Storage, Data Management, Data Exploitation)

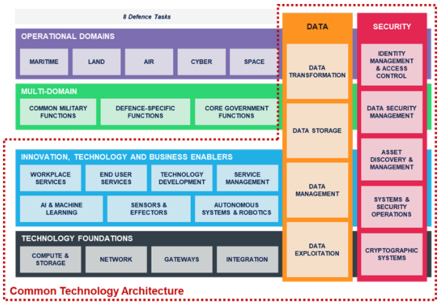


Figure 11 – The Common Technology Architecture (CTA) building blocks

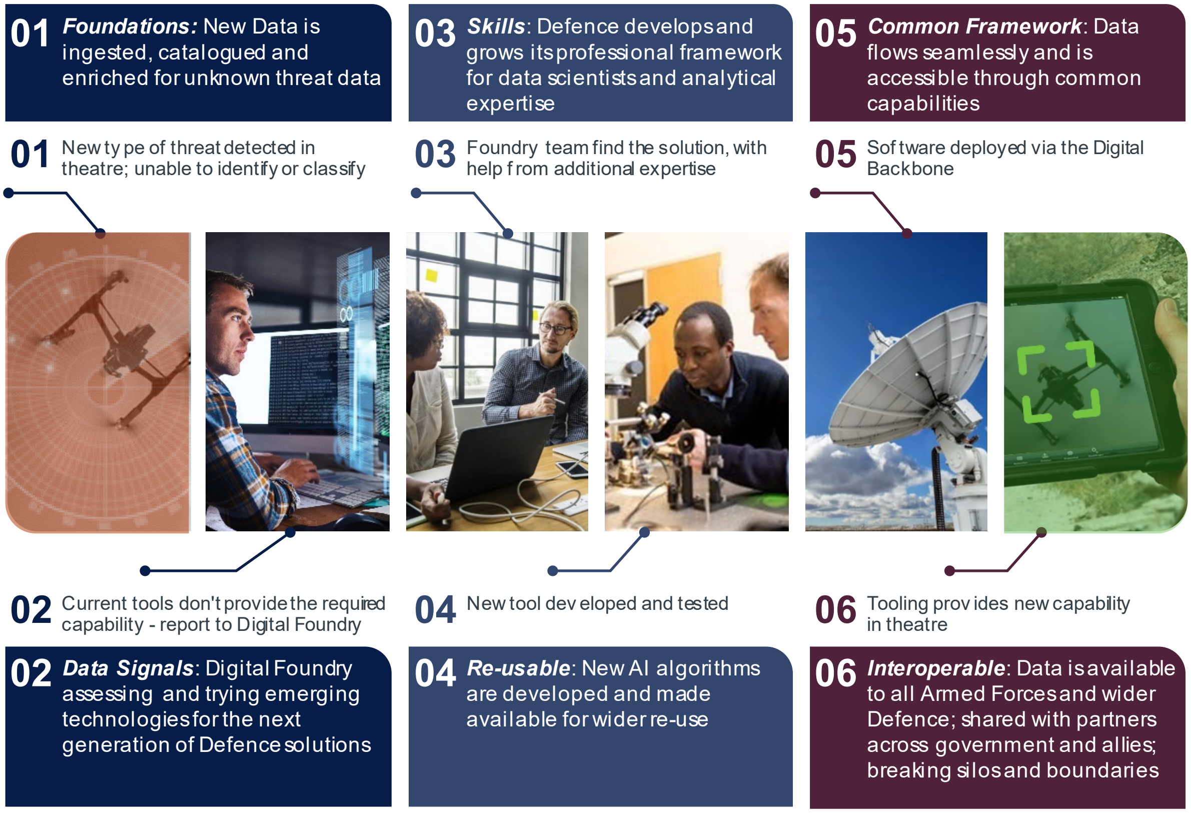
* Please refer to the Common Technology Architecture Blueprint for full details

Annex G: The Digital Foundry and the enabling role of data

The Digital Foundry will be established in partnership with HMG and the best of British industry and academia, to deliver a unique digital exploitation capability for all of Defence. It will also include the Defence AI Centre (DAIC). The Foundry will leverage all Digital Backbone components (people, process, data and technology) to rapidly solve problems and deliver operational solutions to Defence users in near real time.

A key enabler to the success of Digital Foundry is the provision of accurate, reliable and interoperable data to power digital exploitation efforts. The effective capture, analysis and use of data at all security classifications will enable transformative benefits across operational and business environments. MOD's ambition is to build a data-driven enterprise that enables sustainable exploitation through self-service and automation, bringing the customer closer to the point of value realisation.

Data is Central Component of the Digital Foundry Process:



01 ***Foundations:*** New Data is ingested, catalogued and enriched for unknown threat data

01 New type of threat detected in theatre; unable to identify or classify

02 Current tools don't provide the required capability - report to Digital Foundry

02 ***Data Signals***: Digital Foundry assessing and trying emerging technologies for the next generation of Defence solutions

03 ***Skills***: Defence develops and grows its professional framework for data scientists and analytical expertise

03 Foundry team find the solution, with help from additional expertise

04 New tool developed and tested

04 ***Re-usable***: New AI algorithms are developed and made available for wider re-use

05 ***Common Framework***: Data flows seamlessly and is accessible through common capabilities

05 Software deployed via the Digital Backbone

06 Tooling provides new capability in theatre

06 ***Interoperable***: Data is available to all Armed Forces and wider Defence; shared with partners across government and allies; breaking silos and boundaries

Figure 12 - The role of data in enabling the Digital Foundry

Annex H: Exploiting Data to drive value for Defence - Examples

Case Study 1

Project KRAKEN – Supporting Digital Transformation through Data Integration

Project Background

Project KRAKEN has accelerated the development of a fully integrated data platform, bringing valuable and disparate data from numerous systems together on an enterprise scale, and through intuitive workflow and analytics tools is enabling exploitation of previously unknown insights

The Royal Navy and Industry partnership is driving value by integrating key business areas: people, engineering and supply chain. Data as a service, provides integrated, better quality and trusted data for consistent decision-making; resulting in efficient outcomes that drive greater operational value at a fraction of the previous estimated effort. Furthermore, cultural and behavioural changes are organically taking place as engagement flourishes.

Whilst the platform brings the data assets together into a single and secure data integration layer, KRAKEN has automated the process of cleaning, cohering, and managing data, bringing control over the data early on.

Removing efforts on repetitive tasks has allowed personnel to be able to focus on what they were employed to do - make decisions.

By strengthening and simplifying the data curation practices, KRAKEN makes machine-ready data accessible to all. This has democratised trusted data in a reliable environment. Desk-level users without specialised skills can now conduct basic analysis, and those with more skilled or wish to learn have access to suitable tools, e.g. advanced analytics, modelling and machine learning.

> *“By making our data accessible to individuals at every level in the Navy – from Admiral to Able Body – KRAKEN is empowering us as an organisation to better optimise how we operate now, to respond with speed and agility to the challenges of the moment and to understand implications of what we want to be in the future.”*
>
> **Admiral Sir Tony Radakin KCB ADC**

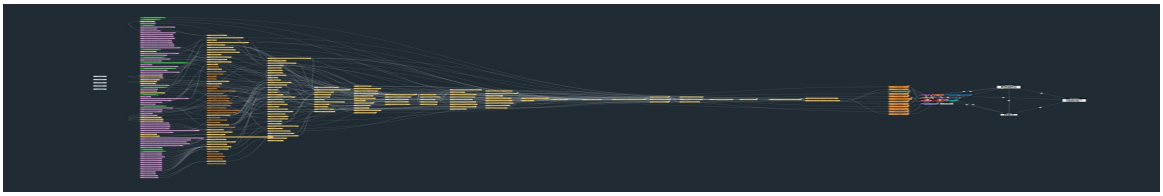


Figure 13 – KRAKEN streamlining data to enable human and machine exploitation

Examples of value realised

Project KRAKEN has delivered significant operational and business value and has encouraged behavioural changes. It has improved understanding of the power of data, data sourcing and transformation practices, and empowered personnel to develop their data skills (through initiatives such as the successfully in-house led JHub Coding Scheme):

- **COVID-19 Response** – To get an instant daily view of the Royal Navy’s capacity (readiness, availability and location) for Covid-19 response deployment, data from the MyNavy app was integrated with the platform, Within 8 days of integration, the daily users **increased from 200 to 27,000 on the MyNavy app**. Senior leadership could provide personnel availability to the Secretary of State for Defence and encouraged improvement at the point of data creation, enabling a behavioural and cultural shift towards data at all levels.
- **Strategic workforce planning** – The platform enabled generation of a simple and dynamic model, allowing the workforce planning personnel in the Navy (c. 60-80 people) to **test assumptions in c. 2.5 hours based on up-to-date data as oppose to around 10 weeks in the past.** Faster iterations of assumption testing enabled faster insight and better investment decisions.
- **Stores contracting** – KRAKEN addressed data latency and allowed the forecasting model to incorporate additional data variables. The effort to forecast costs for stores contracts was reduced from **6 weeks to 20 minutes.**
- **Marine maintenance** – Over-maintenance of assets has been a long-standing Defence issue. Reviewing policies, maintenance behaviours and equipment performance over 20 years, Defence could have **saved 20% of raw maintenance requirement. Over 10 years, this would have saved 97 years’ worth of personnel effort.**

Annex H continued: Exploiting Data to drive value for Defence - Examples

Case Study 2

COVID-19 Response - Online geospatial services

MOD played a key role in supporting the national response to COVID-19.

As part of the Covid-19 response, the Operational Support Team (OST) rapidly designed and delivered bespoke online geospatial services using the Army's cloud-based online analytical platform HYDRA.

An app created as part of the geospatial services to assist with COVID-19 planning was a great success, seeing 1.5mil weekly hits at the peak of activity, with 80 concurrent deployments and a commitment of 11,000 troops.

The success of these services was achieved through having the right people with skills in: scripting, data management and data analysis and Web Geographic Information System (GIS), and a result of leveraging the power of different data sources.

National and government organisations were approached to ingest and distribute data to provide assured, validated and up to date datasets (including geospatial, post code, population, demographic and transport infrastructure data). to develop the apps and layers.

The datasets were assured through a data approvals board (SDAB). This robust system of checking data was essential given the decisions were made based on information presented through the platform.

These geospatial services provided military decision makers and planners with a national common operating picture for Covid-19 and in the first part of 2021, were instrumental in the delivery of Asymptomatic testing sites and the distribution of the vaccine hubs.

Case Study 3

Improving UK Resilience to Plan and Manage Defence Support related to Exceptional Winter Weather

The OST developed a UK-wide weather app and a flood response app to improve the planning and management of exceptional winter weather events in the UK.

These apps have been important for Standing Joint Command (SJC(UK)) and the Joint Munitions Command (JMCs) in response to requests for military assistance and as a planning aid for Vaccine Task Force and commanders 'on task'.

The OST team designed the apps to pull data hourly from a range of sites to provide timely and accurate data on weather, river levels and associated warnings.

The weather app effectively combines a variety of data sources including live river levels, flood warnings, WGBT index, wind speed and direction, EA flood extents and the likelihood impact by County. The 'Flood Response' app uses flood layers with infrastructure and demographic information to enable early and accurate response planning and resource management.

The successful combination of multiple, live, data sources is vital for providing a clear evidence base for the prioritisation and allocation of resources by SJC(UK). It also enables SJC(UK) to better plan for potential requests for military assistance before they are initiated.

Glossary

Glossary (1/3)

Term	Description
Artificial Intelligence (AI)	The simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.
Common Technology Architecture	Deliver common architectural strategy, policies, standards and patterns to increase standardisation and reuse of capabilities, increase interoperability and create a more agile, scalable and networked organisation.
Core Defence data	Data that supports business defined critical Defence processes and operational requirements, and which is shared at the Defence level and/or shared externally or between TLBs, FLCs and/or ALBs.
Data	Collection, storage and exploitation of information in an electronic form.
Data Catalogue	A collection of metadata, combined with data management and search tools, that helps data users to find the data that they need, serves as an inventory of available data, and provides information to evaluate fitness data for intended uses.
Data Centric	Data is available to those who needs, no matter where it is created.
Data Controls Framework	A tool to ensure that all the initiatives, projects and activities within Defence make provisions for the management of data.
Data Estate Map (DEM)	A map of Defence's data. It allows data users to intuitively search the data they need, understand its quality and where it came from, understand the business rules and policies governing its usage, its security classification and the data owner to go to make decisions about that data.
Data Foundations	Standards, practices and policies to build and maintain robust data, preserving and enhancing its value.
Data Management Board (DMB)	1* data board that drives the adoption and implementation of the Data Management Framework, identifying Data Owners and Stewards across the organisations to improve curation practices and quality of the data and delivers data foundational priorities through the establishment of working groups.
Data Mandate	Ensure data is curated, is interoperable and thus delivers effective and optimised data exploitation.
Data Owners	Responsible for overseeing and protecting a data domain (including deciding who has the right to access and edit data and how it's used).
Data Protection Legislation	All applicable data protection laws including the Data Protection Act 2018, UK GDPR.
Data Register	An artefacts that collects information about data assets in an organisation.
Data Rule – Curated	Data is assured, discoverable, interoperable; it is separate from platforms. It is always aligned to the Defence Data Standards & Framework.
Data Rule – Enduring	Data is an enduring asset and capability; it persists beyond individual projects and is continuously maintained to drive military and functional value exploitation.
Data Rule – Exploitable	Defence operates a frictionless operating model that enables sustainable exploitation through self-service and automation, close to the point of value realisation.

Glossary (2/3)

Term	Description
Data Rule – Secure and Digital by Design	Defence Data is robust, fit for purpose, trusted, secured and complies with legal, regulatory and ethical obligations.
Data Rule – Sovereign	Defence takes accountability for its data, knows what it is, where it is, how it is used, sets its policy and is able to assure its adherence to it, regardless of who has custody of it.
Data Rule – Standardised	Defence follows industry, government, data management, and technical standards. The Defence Data Framework provides the artefacts and methods to be applied across Defence in a cohered manner.
Data Rules	6 rules that set out how Defence will treat data and defines what Defence data will look like in future. Data Rules are to be understood, promoted and adhered to by everyone in Defence.
Data Standards	Data standards are the rules around data, from creation through to archiving and deletion of data.
Data Stewards	Ensures the quality and fitness for purpose of an organisations data assets, including the metadata for those data assets.
Defence Data Framework	Provides a single strategic direction for Defence Data across the whole of Defence. For Defence to comply and adhere to.
Defence Operating Model	How MOD works as a whole, how its constituent parts work, how it integrates with the rest of government, and how it works with other organisations (including industry and international partners).
Digital Backbone	Defence's digital infrastructure. A singular, secure, modern and digital environment and an integrated capability approach, a combination of people, process, data and technology; that will enable friction-free access to our data, connecting sensors in one domain to platforms in other domains, via decision-makers at the relevant levels in real time.
Digital Foundry	Including the Defence AI Centre, it will combine new Centres of Expertise (CoEs) in Data, Automation and AI with new teams and skills. It will leverage all of the components of the Digital Backbone (people, processes, data, and technology) to rapidly solve problems and deliver operational solutions to Defence users in real-time.
Enablers	Required to transform Defence into a data driven enterprise, empowering our people with the means to adhere to the rules.
Enabling Organisations	Provide specialist supporting services to the rest of Defence.
Exploitation	Using data to develop insight, power automated processes, control autonomous platforms, analyse our performance and adjust our plans accordingly
Facilitators	Plans to co-ordinate, accelerate and facilitate the Enablers pan-Defence in the delivery of the Strategy. These include delivery plan, metrics and funding.
Frictionless	Without friction, friction-free and achieved with or involving little difficulty

Glossary (3/3)

Term	Description
Fusion	The step that delivers insights, knowledge and intelligence. Knowledge and intelligence can be created from multiple, disparate, fused primary sources Curation includes data fusion.
Hub and Spoke	Organisation design which arranges service delivery assets into a network consisting of an anchor establishment (hub) which offers a full array of services, complemented by secondary establishments (spokes) which offer more limited service array
Hyper-sonics	A hypersonic rocket or missile travels at five times the speed of sound or faster.
Information Reference Architecture	Document or set of documents that provides recommended structures and integrations of IT products and services to form a solution.
Interoperability	Ability of systems and services that create, exchange and consume data to have clear, shared expectations for the contents, context and meaning of that data.
Investment Approvals Committee	Chaired by DG Finance, is responsible for considering major investment proposals on behalf of the Defence Board, forwarding advice to Ministers as necessary on expensive, complicated, innovative, risky, or novel and contentious investments.
JHub Coding Scheme	MOD people teaching themselves digital skills and getting those skills recorded on the system so they can be appropriately deployed. There are currently over 100 military people in the Royal Navy alone who have learnt to code through the scheme (number doesn't include MOD Civilians or other services). Run by UK Strategic Command.
Joint Requirements Oversight Committee	Chaired by the Vice Chief of the Defence Staff, which has been set up to provide additional scrutiny and strongly challenge new capability requirements.
Moonshots	Initial use cases for game-changing technology, with military capability (e.g. machine-speed command and control, predictive sustainment, global status control tower) and business-enabling (HR, Estates etc.) focus
Multi Domain Integration	Multi-Domain Integration. Integrating the 5 domains of air, sea, land, space and cyber and bringing the totality together across a single domain. Integrating across intelligence partners and allies as well as across the totality of the battlespace. MDI is a multi-transformational programme.
Non-Core Defence data	Data that supports intra-organisational reporting, business and operational process. By its nature it never leaves the Function, TLB, FLC or ALB where it was created and is designed for single/few purposes.
Strategic Data Committee (SDC)	3* pan-Defence oversight forum and mechanism responsible for Defence's data outcomes, priorities and requirements.
Strategic Data Steering Group (SDSG)	2* data board that owns the Data Strategy for Defence, assures coherence across all local data strategies, defines Defence Data Priorities and Roadmap and confirms the key Capability delivery programmes where efforts and resources will be focused.

Acronyms

Acronym	Long Title
ABC	Annual Budget Cycle
ACP	Allied Communications Publications
AI	Artificial Intelligence
ALBs	Arm's Length Bodies
API	Application Programming Interface
CDO	Chief Data Officer
CDDO	Central Digital and Data Office
CIO	Chief Information Officer
CSOC	Cyber Security Operating Capability
CTA	Common Technology Architecture
DAIC	Defence Artificial Intelligence Centre
DCO	Defensive Cyber Operations
DDaT	Digital, Data and Technology Profession
DDO	Defence Data Office
DIPS	Digital and IT Professional Services
DISC	Defence Information Steering Committee
DLOD	Defence Line of Development
DOM	Defence Operating Model
DMB	Data Management Board
EO's	Enabling Organisations
FVEY	Five Eyes
FMN	Federated Mission Network
FOC	Fully Operational Capability
GEOINT	Geospatial Intelligence
GIS	Geographic Information System
HMG	Her Majesty's Government

Acronym	Long Title
IAC	Investment Approvals Committee
IOC	Initial Operating Capability
IOC	Integrated Operating Concept
JCN	Joint Concept Note
JMC	Joint Munitions Command
JROC	Joint Requirements Oversight Committee
KUR	Key User Requirement
L&D	Learning and Development
MDI	Multi Domain Integration
MVP	Minimum viable product
NATO	North Atlantic Treaty Organisation
NFR	Non-functional requirement
OST	Operational Support Team
PAG	Partners Across Government
R&D	Research and Development
SDC	Strategic Data Committee
SDSG	Strategic Data Steering Group
SQEP	Suitably Qualified and Experienced Person
SJC	Standing Joint Command
SRO	Senior Responsible Owner
S&T	Science and Technology
TLBs	Top Level Budget Holders
UKStratcom	UK Strategic Command
UI	User Interface
X-HMG	Cross Government

Ministry
of Defence