



Ministry
of Defence

Digital Strategy for Defence

Delivering the Digital Backbone and
unleashing the power of Defence's data



Serving the UK on military operations across the world

April 2021

Introducing the Digital Strategy for Defence

The advance of digital technologies into all areas of society is relentless. It is re-shaping how we live. We instinctively reach for our smartphones, tablets or digital devices to be entertained; to search for information and news; to navigate to unfamiliar places; as well as to communicate with family and friends. The pandemic has accelerated this transformation in our personal and professional lives, and we have all learned new skills and adapted to the changed environment.

In the same way that digital has proved so transformative in our private lives and to so many elements of the private sector, it is also changing the character of competition and conflict at a bewildering rate. Our digital and data networks and devices, protected by our cyber enterprise, are ever more critical to Defence's ability to safeguard our nation's security, stability and prosperity. We need secure access to our data "anytime, anyplace, anywhere" across our sea, land, air, space and cyber platforms, as well as our headquarters and bases, and of course for staff working from their home office. And we must do that conscious of the increasing and ever-present cyber threat from adversaries large and small.

This Digital Strategy for Defence outlines how the Defence Digital Function will enable seamless access to our data by delivering a secure, singular, modern Digital Backbone. It also describes how we will enable the exploitation of that data, across the Defence enterprise, through the creation of the Digital Foundry, a federated ecosystem of digital innovators and developers, which will include a new Defence Artificial Intelligence Centre. Whilst led by Defence Digital, this will be a partnership across Defence, with Dstl and DE&S and the other enabling organisations - all focused on supporting the front-line commands and the wider business of Defence. This is not just about enabling and harnessing new technologies; we need to develop our people, so they are able to embrace and employ this digital technology as easily and intuitively as their favourite social media applications. We need to adapt our processes to access, develop and exploit these technologies in an agile way; as well as ensuring that our data is valued and treated as the strategic asset it is.

I look forward to working with colleagues across Defence, alongside the very best of science and technology, industry, academia, with our partners across government and our allies around the world, to deliver this ambitious and exciting digital agenda.



Jeremy Quin MP
Minister for Defence
Procurement

Jeremy Quin MP
Minister for Defence Procurement

Delivering the Digital Backbone and unleashing the power of Defence's Data

Our world today is unquestionably digital. New technologies from Augmented Reality to Artificial Intelligence (AI) are changing the way we live, and the world-wide pandemic has only accelerated this reliance on technology. The Prime Minister announced in his speech to parliament on the Integrated Review in November last year, that: “our new investment is to be focused on the technologies that will revolutionise warfare”. These technologies – think Automation, AI, Autonomous Vehicles, Virtual Reality, Synthetic Environments and eventually Quantum Computing - will also transform Defence. They rely on huge amounts of data and compute power, seamlessly accessed via the Cloud and secured such that it can be relied upon and trusted.

To meet with the PM's intent, we will work with our UKStratCom colleagues and the Digital CIOs across Defence to build the underpinning Digital Backbone that will enable the revolution of warfare and the transformation of Defence. This Singular, Modern, Secure, Digital Backbone will connect our decision-makers across our military and business domains, to enable faster, better decisions and improved Defence outcomes. While the Backbone will give seamless access to our data, the real game-changer is unleashing its power through ruthless exploitation. Therefore, although our plans are still in their infancy, we will seek to pull on the very best of Defence, S&T Industry, Academia, Partners and Allies to develop a new Agile Software Development Centre or Digital Foundry.

Our digital ambition is not limited to the introduction of new technology. That may be the easy part as much is commercially available. Our challenge is to ensure all in Defence have the digital skills to manipulate the technology; that our processes are agile and streamlined and we have our data in the right quantities and format to exploit.

This Strategy outlines how the Digital Function will enable Information Advantage, Multi-Domain Integration and the principles described in the Integrated Operating Concept. The Backbone, enabling the shift to operate and persistent engagement, will abide by NATO and cross government standards and will set the digital and data “Rules of the Road” for all. While there is obvious connection to those directly employed within the Function, as a critical enabler to other Defence Functions, HLBs and FLCs, this strategy should be read by all as we are all touched by Digital, Data and Cyber activities. Moreover, if we are to truly revolutionise warfare and transform Defence, all will need to lead and adapt to the more agile and flexible ways of working Digital will provide.

As the digital world rapidly changes so too will our assumptions. We will iterate and refresh our strategy within 18 months, and further expand on how we will build the new Digital Foundry. As the great Charles Darwin once wrote “It is not the fittest, nor the most intelligent that survives. It is the most adaptable to change.” Perhaps if alive today, he would have amended to “most adaptable to *digital* change”!



Charles Forte
MOD Chief Information Officer
Digital Functional Lead

A handwritten signature in black ink that reads "Charles Forte". The signature is written in a cursive, flowing style.

Preface

“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

Purpose

This Digital Strategy outlines the step-change in approach that is required for Defence to leverage Digital and our Data, as fundamental enablers, to facilitate faster, better decisions and improved Defence outcomes.

Placing a Digital Backbone at the heart of the approach, this strategy describes what needs to be in place to build the backbone, as well as to enable and accelerate exploitation across Defence, in order to enable Defence Priorities. It matches these Ways with the Means required to meet the Defence’s Digital Ends. While this iteration of the strategy has a deliberate and necessary focus on building the enablers at this stage, its successor will describe Exploitation in more detail.

This is a whole-Digital Function Strategy, not constrained to the Defence Digital organisation, but recognises the boundary with weapon systems and platforms, control systems, Operational Technology and networked non-Information Technology systems.

Audience

The strategy provides guidance and a clear signal of intent to staff and decision-makers across the Digital Function – Commands, Functions and Enablers.

Given the critical dependency on Digital across Defence, the readership is deliberately broad and includes those involved in the Governance of Digital – members of the Defence Information Steering Committee, Defence Delivery Group, UK Strategic Command Executive Committee, and the Digital Functional Coherence Board. It should be read by Customers – those who commission services, and Users of those services, as well as our partners across Government, international allies and suppliers.

Linkages

This document supersedes and replaces both the Digital & IT Functional Strategy (Jan 19) which signalled the establishment of the Digital Function, and Enabling Warfare in the Information Age (Dec 19) which described the steps being taken to build functional capability.

It is coherent with the aims of - and should be read in conjunction with - the Integrated Operating Concept 2025, and is the capstone document to extant and forthcoming Digital Function sub-strategies¹.

¹Including subordinate strategies on Data, Cloud, Exploitation, 5G, Sustainability

Contents

Part 1 - Strategy

01 Ends

- 8 Context and Diagnosis
- 10 Our Vision
- 11 Strategic Outcomes

02 Ways

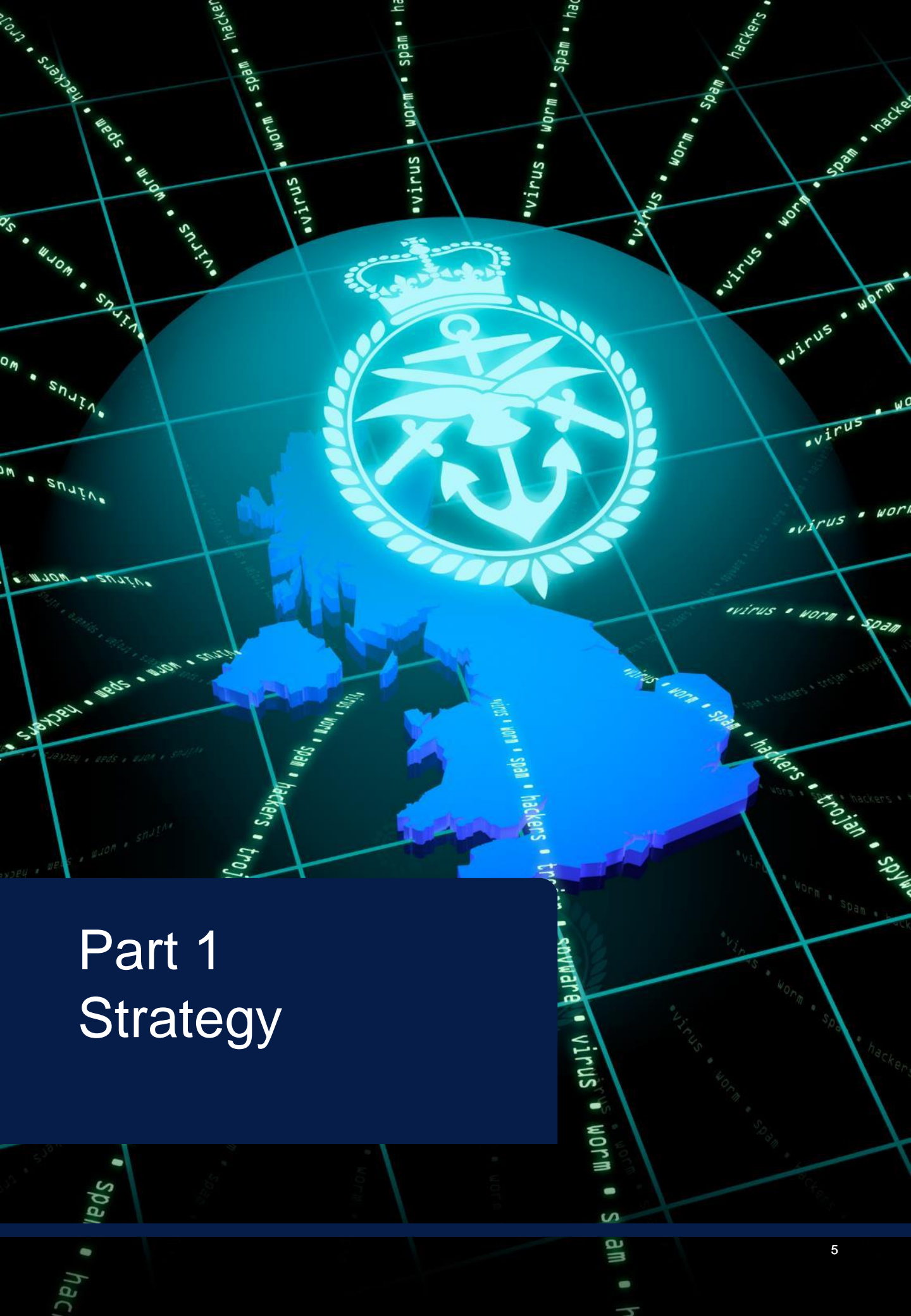
- 14 The Digital Backbone
- 16 People
- 18 Process
- 20 Data
- 22 Technology
- 24 Securing the Digital Backbone
- 26 Exploiting the Digital Backbone
- 28 Integrating the Digital Backbone

03 Means

- 30 Implementing the strategy
- 31 Delivery
- 32 Investment and Benefit

Part 2 – Operating Model

- 35 CIO Accountabilities and Authorities
- 36 Operating Model construct and processes
- 37 Senior Leadership Accountabilities
- 38 Governance



Part 1 Strategy

Summary of Defence's Digital Strategy

Diagnosis: where Digital is today and why

Digital is all-pervasive and is changing the character of warfare and politics, as data-driven capabilities change the way we communicate, live, work and compete. This brings both opportunities and threats. To deliver the Defence Purpose in an era of persistent competition, we must adopt a new approach to grasp the opportunity of disruptive technology; we must also address legacy issues that prevent exploitation and new ways of working. Specific issues include:

- Our data is fixed inside internal and contractual silos and is hard to access and integrate
- We have critical digital skills gaps across the enterprise
- The technology core is too fragmented, fragile, insecure and obsolescent
- We remain mired in industrial age processes and culture

We have a core digital programme but critical components are missing. The Digital Function must transform, enabling Defence's wider transformation. Ultimately it must enable Defence to be integrated across all five Domains, integrated nationally, engaged internationally, with a more assertive and adaptable Defence posture.

Vision: where Digital needs to be by 2030

- Defence will value Data as a strategic asset, recognising it as the mineral ore that fuels integration and enables a system-of-systems approach.
- We will persistently deliver transformative Digital capabilities to enable sustainable military and business advantage.
- These capabilities will be secure, integrated, easy to use and delivered at scale and pace to all in Defence.

Strategic Outcomes: where Digital needs to be by 2025

- A secure, singular, modern Digital Backbone is connecting sensors, effectors and deciders across military and business domains and with partners, driving integration and interoperability across domains and platforms.
- Enabled by the backbone, a Digital Foundry is unleashing the power of Defence's Data, exploiting Artificial Intelligence and other game-changing technologies.
- An empowered, skilled and agile Digital Function is driving Multi-Domain Integration and Defence Transformation.

Data exploited at scale and speed

Data accessed and used as a 'strategic asset' in conjunction with the tech game-changers, delivered at scale and pace

Right talent in a single unified Function

Leading-edge skills in partnership with UK industry and academia; a single, capable Function to drive the strategy

Cyber Defence reset

Defence's systems and assets are secure by design and resilient to attack, with intelligence-led dynamic risk management

Modern technology platform delivered

A single technology Backbone to support integration, platform interoperability and operational speed.

A step-change in Digital delivery

Capability that is relevant to the need, easy to use, works reliably, is cost-competitive and delivered on time

Ways: initiatives to achieving our strategic outcomes

Delivery requires a strongly co-ordinated and integrated pan-Defence approach, with action taking place in a federated approach across the Commands, Enabling Organisations and Functions. Culture change and an agile approach are absolutely key. The Digital Function will continue to build professionalism, skills and the internal mechanisms to be able to act cohesively. We will work in close partnership with Multi-Domain Integration in Strategic Command, with wider Transformation and other Functional change programmes.

People – Upskilled workforce within one Functional Operating Model

- ✓ Upskilled people
- ✓ Effective partnerships
- ✓ A single Function acting together to drive the strategy

Process – Coherence for 'One Defence'

- ✓ Transparent portfolio
- ✓ Common standards
- ✓ Enterprise-wide IT Operations
- ✓ IT supply category management
- ✓ Controls

Data – Using Data Strategically

- ✓ Data is catalogued, accessible, useable
- ✓ Digital Foundry: AI, Robotics, Synthetics at scale
- ✓ Design shift from Platform-centric to systems-centric

Technology foundation

- ✓ Multi-class hyperscale cloud
- ✓ Next-gen resilient network
- ✓ Obsolescence management
- ✓ Common architecture
- ✓ Modern services

Cyber – Defence

- Resilience and Operational integration
- ✓ Key gaps closed
- ✓ Capability upgraded
- ✓ Secure by design
- ✓ Compliance
- ✓ Cyber awareness
- ✓ Detect & Respond expanded

Our guiding principles for the Digital Function are:

Cohesion: a strong single Function that works to a common functional plan and aligning processes

Speed: working with new levels of agility to turn ideas into delivery at scale

Integration: common architectures and standards driving design and delivery integration by default

Business Rigour: new levels of discipline and rigour in how we work to deliver and assure outcomes



01 Ends

Context and Diagnosis

The world is changing – Digital is at the heart of this and Defence must pivot.

We are living in an era of accelerating technological change - everywhere we look data-driven capabilities are changing the way we communicate, live and work. We are becoming increasingly empowered by, and dependent on, digital technology.

This creates both opportunities and threats, as our opponents proactively seek to exploit the same tools at our expense. Given the widespread availability of these technologies, advantage will come from their rapid adoption and imaginative exploitation through new ways of working, operating and fighting.

“The pervasiveness of information and rapid technological development have changed the character of warfare and politics”

***General Sir Nick Carter,
Chief of the Defence Staff***

In an era of persistent competition, we must adopt a more agile approach to place the latest technologies in the hands of our operational and business users, whilst ensuring our people, processes and data keep pace with best practice.

Defence is firmly grasping the challenge of this disruption – both opportunity and threat – at the most senior levels and Digital sits at the heart of our developing investment options.

The Digital Function is a critical enabler to the Defence Operating Model – Digital capabilities provide the connective tissue enabling Multi Domain Integration and Transformation

Our ambition is to multiply the national advantages we enjoy. An advanced digital economy; a strong entrepreneurial base; a committed and mobilised Defence workforce of civilians, reserves, regulars and partners across industry and academia. The Covid-19 pandemic has accelerated our familiarity and desire for digital flexible ways of working.

The benefits that would accrue from bold investment include an affordable asymmetric edge over our competitors; Tier One ‘reference’ status with our Allies; and the opportunity to run the business of Defence with greater accuracy, speed, productivity and efficiency.

It is also an opportunity to partner and innovate with the Science and Technology community, other Departments and the UK technology industry in new ways that provide mutual advantage, supporting the UK brand, promoting prosperity, projecting influence, enhancing our resilience and, equally important, to play our part in reducing the UK’s carbon emissions.

Digital is one of 16 Functions across Defence, and one of the central Functions that are aligned across Government. Functions ensure the proper delivery of Defence Outputs and are primarily about ensuring coherence across critical activities in support of Military Capability.



“The standardisation of our networks, information exchanges and data, Defence’s digital backbone, is the critical enabler to integration across everything we do”
General Sir Patrick Sanders,
Commander Strategic Command

We must, however, address some key constraints

Defence’s existing IT core has grown organically over many years, with ever-perpetuating technology debt and security vulnerabilities. We are not yet exploiting emerging technologies at pace and scale.

We have too often traded-out technology refresh and have not driven sufficient integration and commonality. Continuing down this path will prevent us from exploiting emerging technologies at the pace and scale required to deliver the Defence Purpose.



The technology core is too fragmented, fragile, insecure and obsolescent



Data is fixed in internal silos, and difficult to access and integrate



We have critical digital and data skills gaps across the enterprise



We remain mired in Industrial-Age processes and culture

We have a core digital programme but critical components are missing across People, Process, Data and Technology. There are particular gaps in hyperscale Cloud capabilities at all classifications.

We must ensure that Digital enables Defence to be integrated nationally, engaged internationally, with a more assertive and adaptable Defence posture, and Information-led.



Our Vision

It isn't enough to just do the same things better and faster; to truly grasp the opportunity we have to make some deeper and more fundamental shifts.

Our Vision out to 2030

Defence will value Data as a strategic asset, recognising it as the mineral ore that fuels integration and enables a system-of-systems approach. We will persistently deliver transformative Digital capabilities to enable sustainable military and business advantage. These capabilities will be secure, integrated, easy to use and delivered at scale and pace to all in Defence.

We need data-driven, inter-connected digital systems, that can integrate easily and securely with our partners across Government and our allies, and where 'software defined capability' gives us an asymmetric edge by sensing, recognising and responding to new opportunities and threats faster than our adversaries.

This means connecting Defence not just across Sea, Land and Air, but also the emerging domains of Space and, Cyber and Electromagnetic, as well as partners across Government and allies over-the horizon and across the world. It is not just about 'doing things better'; it is also about 'doing better things'.

We will put in place the enablers to allow digital exploitation for critical MDI programmes, including those delivered through the 'Moonshots' programme. This must enable the ability to share information and data across platforms and domains: sensors connected to effectors, via appropriate decision-makers.

This same approach will transform our corporate activity, generating significant efficiencies in time, cost and workforce and driving more flexible ways of working, designed around user needs. It will allow us to automate core processes and unlock the value in our data to make better, quicker, evidence-based decisions. This digital capability will allow us to transform other horizontal Functional areas such as HR services, Acquisition and Support and release Defence's people into higher value roles.

Over the next 10 years we plan to **invest an additional £1.6bn** in People, Processes, Data, Technology and Cyber

Digital & IT Transformation
enables (and is enabled by)

Support, People and Acquisition Transformation

which together with TLB programmes deliver

Efficiencies (financial, workforce, time)
that can be reinvested into

Data-driven, software-enabled military capabilities

that are powered by

Experimentation, Research & Development
and exploited by

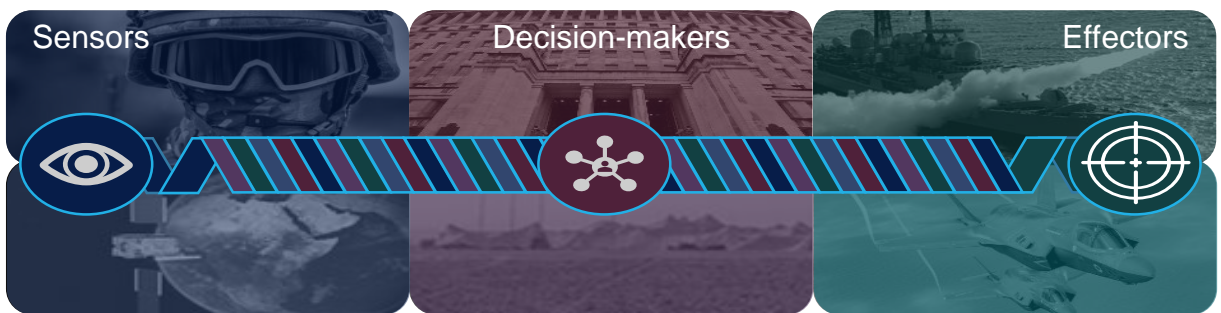
Agile Ways of Working and Operating / Fighting
all cohered by an

Integrated Operating Model
to deliver

The Defence Purpose

Strategic Outcomes

Our plan is a twin track integrated and iterative approach – We will accelerate Digital exploitation and build a modern Digital Backbone to support it.



Where Digital will be by 2025

A secure, singular, modern Digital Backbone is connecting sensors, effectors and deciders across military and business domains and with partners, driving integration and interoperability across domains and platforms.

Enabled by the backbone, a Digital Foundry is unleashing the power of Defence's Data, exploiting Artificial Intelligence and other game-changing technologies.

An empowered, skilled and agile Digital Function is driving Multi-Domain Integration and Defence Transformation.

"Multi-domain integration is the posturing of military capabilities in concert with other instruments of national power, allies and partners; configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains and levels of warfare" – *Joint Concept Note 1/20: Multi-Domain Integration*

Data exploited as an asset, at scale and speed – Data accessed and used as a 'strategic asset' in conjunction with the tech game-changers, delivered at scale and pace.

The right talent within a single unified Function – Leading-edge skills in partnership with UK industry and academia; a single, capable Function to drive the strategy.

Cyber Defence reset – Defence's systems and assets are secure by design and resilient to attack, with intelligence-led dynamic risk management.

Modern technology platform delivered – A single technology Backbone to support integration, platform inter-operability and operational speed.

Step-change in Digital delivery quality achieved – Capability that is relevant to need, easy to use, works reliably, cost-competitive and delivered on time.



“We must become data-centric and exploit the data that we collect”

General Sir Patrick Sanders, Commander Strategic Command

Unleashing the Power of our Data

While the Digital Backbone is the enabler, it is the **exploitation of our data** that will revolutionise warfare and transform defence. Our AI Delivery Centre, as a key game-changing component of the Digital Foundry, will be at the centre of this.

Defence’s vision puts modern digital capability at the heart of how it operates. The effective capture, analysis and use of information at all security classifications will enable transformative benefits in the operational and business environments. Achieving these benefits requires common, interoperable, standardised data and data services, which are actively managed, curated and governed.

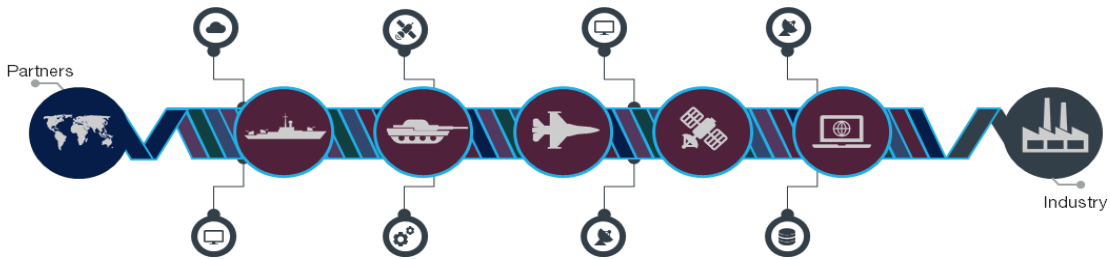
Our aim through the Digital Backbone is to **exploit our data across Defence** and drive value through:

- ✓ **Faster decisions supported by trusted insights** – enabling the frontline forces to have real-time access to data they need from across the battle space and business space, for faster situational awareness and decision making. This includes the persistent access to digital and data services for our globally deployed forces, operating below the threshold of warfighting.
- ✓ **Efficient and effective planning** - logistical planning and operational readiness rely on trusted insights from across our supply chain and people. Organisation-wide integrated data will ensure Functions and operations are reliably informed.
- ✓ **Using advanced analytics to secure military and business advantage from our data** – recognising that data is both an offensive and defensive weapon, and using analytics and AI capabilities to drive new insights and understanding to stay ahead of our adversaries.
- ✓ **Transforming our operational capability** – driving Multi-Domain Integration and collaboration in the battlespace: “connecting any sensor to any effector via any decision-maker”.
- ✓ **Accelerating programmes and transformations** – seamless data flow across organisation boundaries will underpin our ability to successfully deliver the large, complex programmes which improve our military and business capabilities.



02 Ways

The Digital Backbone



“Warfare will be enabled at every level by a **digital backbone** into which all **sensors, effectors and deciders** will be plugged”

General Sir Nick Carter, Chief of the Defence Staff

Defence’s Digital Backbone will be an ecosystem – a combination of people, process, data and technology; it 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.

A 21st Century Digital Backbone is critical to enabling Multi Domain Integration and Defence Transformation.

The Digital Backbone must be designed around how Defence wants to operate and fight¹ and how it intends to function as a Department of State (set out in the Defence Operating Model) - and not be driven through a narrow technology lens.

With continued investment a modern Digital Backbone will deliver data-driven, inter-connected digital systems that integrate across domains, partners, allies and suppliers.

This approach will transform not just our front-line operations but also our corporate activities, maximising efficiencies in time, workforce and cost to be reinvested where they are most valuable.

This allows the rapid exploitation of that data by increasingly sophisticated tools, to develop insight, power automated processes, control autonomous platforms, analyse our performance and adjust our plans accordingly.

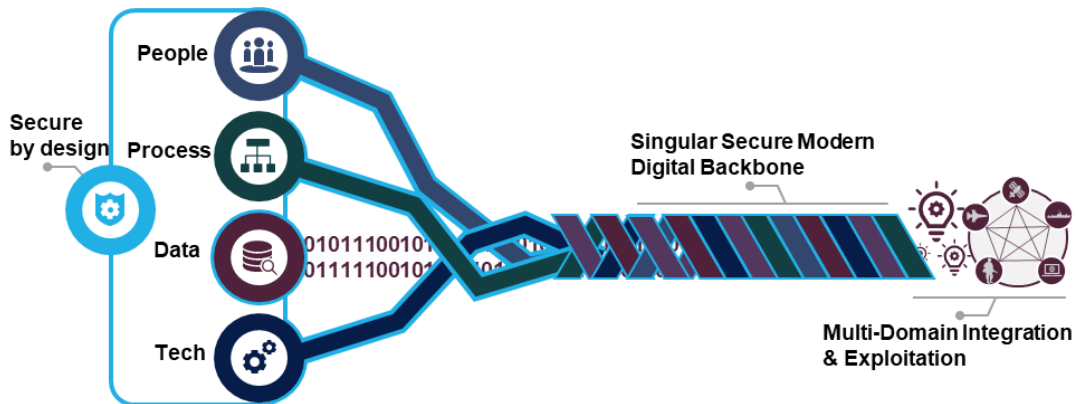
It will allow us to sense, recognise and respond to new opportunities and threats faster than our adversaries, getting the best out of the ‘sunset’ systems we have, as well as underpinning future software-intensive ‘sunrise’ capabilities.

The Digital Backbone will be:

- ✓ **Singular** - delivered by an increasingly qualified and cohesive workforce, based on common standards and architecture across the breadth of Defence, directed and assured by the CIO.
- ✓ **Secure** – to protect and defend Defence’s data, networks, systems and decisions.
- ✓ **Modern** – cloud-based and iteratively incorporating emerging technologies.
- ✓ **Digital** – allowing Defence to exploit curated data as a strategic asset and enabling a strategic shift to software-intensive capabilities that provide sustainable and affordable competitive advantage.

¹IOpC25, MDI JDN

A Singular Secure Modern Digital Backbone for Defence



Secure by Design, with People, Process, Data and Technology woven through it



Effective exploitation and the Digital Backbone are as much about humans as about data and technology, and strengthening our capability in a number of ways is the foundation we must build. Diversity and the inclusive working environment fosters ideas and innovation.

A strategic workforce transformation programme for our People capabilities



We must rethink long-held mindsets and processes to put the right governance in place in key areas of design, investment planning, programme delivery and also how we manage the information environment to ensure operational integrity and the free, resilient flow of data.

Digital programmes under one design, one architecture, one system



Data is the mineral ore that drives Defence and we need to be far more thoughtful about both internal and external sources and uses. Design will be based on an understanding of where data needs to be created, accessed, integrated, secured and consumed.

Data deployed as an asset across data-driven, connected digital systems



The core technical building blocks are the networks, gateways, hosting services, user interfaces (including identity management and access mechanisms) and middleware that come together to deliver data and information wherever and however we need to exploit it. Delivered through Strategic Command and TLB Equipment Programmes.

Hyperscale Cloud, Next Generation Networks and Modern User Services

Access to, and control of, the Electromagnetic Environment is essential to all operations and to the functioning of the Digital Backbone¹. The cyber terrain is more than just IT and copper or fibre networks, and with the advent of 5G and Internet of Things, will grow far faster and wider in the next few years. As such, data and architectural standards, as well as management of the EMS, will secure operational advantage and freedom of manoeuvre.

¹ FEMA JCN 2/21

People



The Digital Backbone is as much about People as it is about data and technology. Effective delivery and exploitation of the Digital Backbone requires us to transform our workforce and develop and embed digital skills across Defence.

We need to keep pace with the increasing capabilities of our adversaries and we have fallen behind in accessing the specialist skills we need. Demand for these skills is high and the market for them is very competitive. To compete we need to maximise our brand, offer real and unique learning experiences, and invest in the development of our people.

But acquiring the technology talent to build the Digital Backbone won't be sufficient – realising its full potential requires us to foster an environment where people are able to find new ways to exploit the technology across the operational and business domains. We need a more agile, risk-taking, flexible and innovative culture which encourages creativity and diversity of thought, backed up by multi-disciplinary teams to turn ideas into outcome delivery.

To this end, Defence Digital is transforming how it operates, and building a workforce with the skills required to match our ambition to deploy the Digital Backbone and exploit it effectively across Defence.

What is needed to deliver the Digital Backbone



A transformed workforce

The right skills, roles, and mix of people in Defence Digital



A highly skilled Digital Function

Investment in our people to deliver a professionalised, interoperable workforce with the Digital capabilities we need



A digital culture across Defence

An educated and digitally savvy Defence

“In an increasingly digital competition, we all need to individually play our part in stepping up, upskilling and practicing our digital art and tradecraft if we're to win against increasingly sophisticated adversaries”.

Air Vice-Marshal Ian Gale, Assistant Chief of the Air Staff

How we will deliver the People capabilities we need:

Our Strategic Workforce Transformation Programme sets out how we are transforming our People capabilities. We will:

1. Transform our Defence Digital HLB workforce to deliver the Digital Backbone

We are investing in a Whole Force approach to build the right organisation at the core of the Function. This will transform Defence Digital into an efficient organisation with the right skills to become a highly capable and technically skilled workforce, including new skills in areas such as Data & Analytics, Agile delivery and cyber. We will optimise how we access the market for critical and niche skills to deliver a flexible organisation with the right balance of Crown and contractors to meet our changing demands. And we will develop how we attract and retain talent to ensure we have the right people to drive the culture, leadership and behaviours we need.

2. Professionalise the Function and create an interoperable workforce

We will develop the Defence-wide Digital and Information professions¹ to provide a common professional development framework. We will manage the profession as a single cadre with clear standards, career paths and a common talent management / development process. To drive interoperability across the Function we are adopting a common onboarding process and aligning career pathways to all 3 cross-Government profession capability frameworks – DDAT, Cyber Sec and KIM. We will continue to strengthen our talent pipeline through secondments from across government, industry and academia, and improving and expanding Apprenticeships and Graduate schemes to grow talent internally.

3. Enable a Digital mindset across Defence

We will embed digital skills and ways of working across Defence via the Digital Academy² through:

- Investment in a new Digital Platform and Learning Service to upskill our workforce
- Learning initiatives to increase Digital awareness pan-Defence and give people the confidence to use data and technology appropriately
- Making a step change in ways of working – cutting through processes and layers of control, making it easier to work with the core function and bringing us closer to the demands of wider Defence

What this will deliver for Defence

Digital capability embedded throughout the Function, giving us the tradecraft to deliver and exploit the Digital Backbone and foster a more digital mindset throughout Defence

A more efficient Function through a lean organisation, removal of duplication and clarity of accountabilities, and the ability to respond to variable demand

An upskilled workforce to deliver our digital ambition:

- Effective delivery of core services, improved responsiveness to operational requirements and confidence in Defence Digital's capability to deliver for our customers
- Faster delivery of value to Defence, through a modern organisation trained in modern digital delivery methods

Opportunity to inspire Digital professionals to develop their career within Defence

¹Digital Data and Technology (DDaT), Cyber Security and Knowledge and Information Management(KIM)

²The Digital Academy provides services to enable the workforce of the future – connecting people and opportunities, unlocking the potential for the future workplace, and developing meaningful careers with the Digital and Information professions

Process



Embedding and driving the right processes will enable the singular Digital Backbone – our vision is for a more coherent Defence with common standards, governance and processes realising One Backbone for One Defence.

Given the exponential rate of change, setting the correct processes for the design, delivery and operation of the Digital Backbone is critical – too much structure stifles innovation and experimentation, but too little leads to chaos and inefficiency.

Where we set and uphold the right standards¹ for data, technology, cyber and people, they will drive the right priorities for all of Defence by enabling greater integration, interoperability and economies of scale. They will also allow for successful developments to be scaled and shared across the enterprise.

What is needed to deliver the Digital Backbone

Maturing the Digital Function processes

Consistent **People capabilities**

Strong Functional Management
(Performance & Portfolio)

Governance against common standards

Enterprise-wide IT Operations processes delivering greater connectivity, automation and information exploitation

To achieve our vision for the singular Digital Backbone, we must strengthen our horizontal integration to drive consistency, cohesion and integration in a number of areas:

- **People** – co-ordinate Digital skills, capacity and development planning, providing the right balance of people capabilities to deliver the digital backbone.
- **Functional Management** – strengthen our management processes and controls, through the Functional Portfolio and underpinned by functional performance and governance, to deliver coherent investment aligned to strategic intent.
- **Data** – drive the data mandate and authority on programmes, data resources and governance.
- **Technology** – Powerful, federated governance mandating adherence to a 'Single IT Road System' of common architectures and standards.

¹Related Digital policy, rules and guidance hosted on Defnet at following [link](#).

Establishing the Enterprise-wide IT 'Rules-of-the-Road': the Single IT Road System

There is increasing need for information to flow and to be accessed end to end across Defence. This means we need to treat our IT infrastructure as a single entity and manage it in a consistent way. The current lack of end to end visibility, poor awareness of what is place and an inability to apply controls presents a huge risk and is not an acceptable position. We are compromised with respect to security, operational integrity, functionality and speed.

Therefore we will improve our approach to IT Service Management and Integration to deliver a clear view of the IT infrastructure and the technology components it comprises, how it is connected and how it is managed across Defence. This will ensure that we keep the Digital Backbone operating successfully through clear and enforced operational rules of the road, including patching, configuration, change, incident and problem management.

Improving how we Deliver and Operate for Defence

Some critical outputs are under pressure and the general digital environment is becoming more challenging. A combination of inadequate internal business performance controls and MI, strain associated with supporting an unconstrained demand signal (both operational and Equipment Programme) and an ever-increasing technology debt lead to the requirement for interventions.

We are addressing these challenges and driving improvements in IT programme delivery and multi-domain integration through the SDO Reset Programme which includes:

- ✓ Upskilling to focus on end-to-end service accountabilities;
- ✓ Professionalisation of project delivery;
- ✓ Improvements to core service performance;
- ✓ Supporting MDI through agile Cyber C2 and Cyber Mission Assurance;
- ✓ Creating insights and driving action through resetting controls and using effective risk and MI;
- ✓ Improving effectiveness and efficiency through economy-of-scale approaches to 3rd party costs
- ✓ Improving supplier engagement via Strategic Supplier Management

What this will Deliver for Defence

The Digital ambition for Defence will be achieved through coherent and complementary strategies across the TLBs and Functions with architecture setting the technical strategy for Defence.

Enabling organisations will deliver interoperability and maintain Digital capability by working to common standards; they will be able to align investments and suppliers, achieve common Digital objectives and build solutions which can be shared and exploited pan-Defence.

IT Operations across Defence will be managed according to a single IT Road System, enabling greater connectivity, automation and information

exploitation.

All new technology investments across Defence will be tested against alignment and compliance to policies and standards.

Digital risks will be managed holistically to decrease the likelihood of impact on achieving Defence Outputs.

Digital investment across Defence is efficient, coherent and aligned to deliver strategic intent

Defence's Digital profession is equipped with the right people and skills to deliver.

Digital leadership is held to account to deliver shared Digital ambitions.

Data






For MOD to gain strategic military advantage on the battlespace and to drive efficiencies in the business space we must exploit our data to the fullest. Effective management, coherence and standardisation of data pan-Defence is central to the success of the Digital Backbone and a critical enabler of Multi-Domain Integration.

Defence has the capacity to capture huge volumes of data but the lack of adherence to common rules inhibits our ability to exploit it at the tempo necessary to achieve advantage. We do not have the required capabilities and structures to drive benefits from data – we are missing enterprise and ecosystem collaboration and we lack the basic foundations to fully curate and exploit our data assets. We need the ability to make key business and battle space decisions that are based on trusted and timely data that is available and accessible to all that need it, when they need it, regardless of geographical, platform or organisational boundaries.

What is needed to deliver the Digital Backbone

Defence is on a transformational journey to become a data-enabled organisation that leverages data as a strategic asset. We will have interoperable, standardised, machine-ready exploitable data and data platforms across Defence to drive value through optimal exploitation. To achieve this we need to:

-  **Establish Data fundamentals**
 - Foundational capabilities and standards for data curation and management
 - Data Governance framework and controls to establish data authority
-  **Optimise and cohere across Defence**
 - A unifying function that drives commonality of tooling and methods for exploitation excellence
 - Collaboration with Partners across Government, international allies and National Security partners
-  **Drive exploitation**
 - Game changing data technologies & analytics, data science and Artificial Intelligence capabilities delivered at optimal cost and efficiency

How we will transform Defence into a Data-enabled organisation

Fundamental to addressing our challenges is the establishment of MoD Data Rules¹ to underpin all aspects of data capability, governance and delivery pan-Defence. These rules set the criteria and standards against which all data delivery and decisions across Defence will be measured:

- a. **Sovereign:** Data will no longer be held or hidden in silos – we will know what our data is and where it is.
- b. **Enduring:** Data will be treated as an enduring asset, recognising that it persists beyond individual projects and will be continuously maintained.
- c. **Curated:** Data will be managed in a consistent manner throughout all stages of its lifecycle ensuring its adherence to standards, availability, accessibility and fitness for purpose.
- d. **Standardised:** Data will follow industry, Government, management and technical standards.
- e. **Exploitable:** Data will be close to the point of customer value, enabled by a frictionless business model for sustainable exploitation.
- f. **Secure and Digital by Design:** Data will be trusted, secured and compliant with legal obligations. Data will no longer be an afterthought and will be an essential part of all programmatic delivery.

To embed these data rules and realise benefits at pace we will:

1. **Deliver the MOD Data Strategy:** The Defence Data Office will define the Data framework for the management, governance and exploitation of Defence Data assets, enabling a coherent approach to innovation, standardisation and opportunities for exploitation and bringing alignment for Defence to work together effectively. We will partner for data excellence, advantage and true integration with our Partners across Government, Allies and partner organisations in industry and academia through coherent data standards, commercials and tooling.
2. **Build the Data Fundamentals:** We will professionalise the management of our data assets by building the data standards and artefacts that Defence will adhere to. We will know what is our data, where is it, who owns or curates it (for example Data Catalogue, Information Architecture).
3. **Embed Data Controls and Governance:** We will formalise the decisions made across Defence for the management and use of its data assets. Data will have a seat at the table of Defence's functional governance structures responsible for the strategy, investment and release-into-operation of all our programmatic and transformational delivery and our day to day data management practices.
4. **Drive Advanced Data Exploitation:** We will deliver the standards and best practice for the exploitation of Defence Data assets. We will release an operational AI Analytics environment designed to rapidly scale and innovate using advanced technologies. We will optimise the exploitation model to enable access to data and its interoperability across domains.

What this will deliver for Defence

A curated, trusted and interoperable data asset, supported by a consistent and common approach available for exploitation close to the customer

Strategic programmes accelerated by availability of standardised machine and exploitation-ready trusted data, and the right expertise to support

Improved pace of innovation and capability deployment to operational and business users that is led centrally and delivered through common federated goals

Modern expertise and capability in AI, Analytics and Data Science to identify and exploit newer sources of battlespace and business insight

¹Data Rules published in the MOD Data Management Strategy

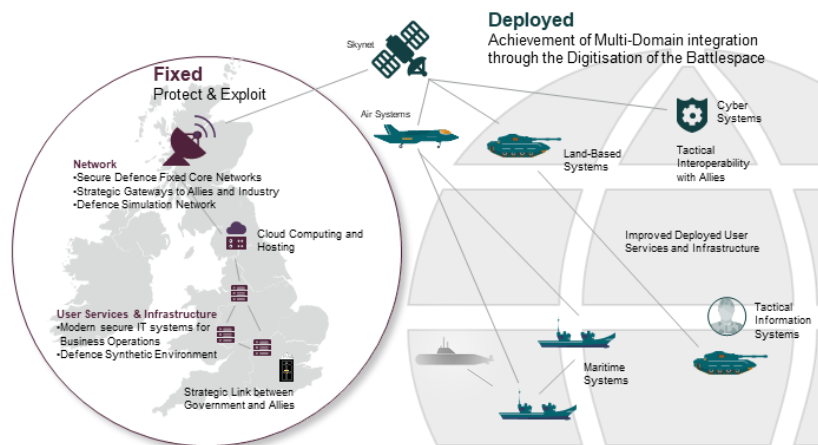
Technology



In the future, technology will be the backbone of a truly integrated force – but today, a significant proportion of our technology systems are fragmented, fragile and obsolescent.

Continuing on this path will perpetuate risks, costs and a lack of interoperability which Defence can simply no longer tolerate. Instead, we must migrate users on to a modern, secure technology foundation which enables Defence to better exploit the value of emerging technologies.

Technology, and the processes that support it, are also fundamental to ensuring the Digital Backbone is singular. We must replace our siloed legacy services with a robust, common Digital Backbone – designed for all of Defence.



What is needed to deliver the Digital Backbone

We will build and exploit a single modern Digital Backbone for Defence via uplifts to our existing services and capabilities in three main areas;

- **Hyperscale Cloud**¹ – providing the foundation for us to build and deliver the future capabilities we need across all classifications.
- **Next Generation Networks**² – allowing seamless access to data and enabling easier collaboration with our allies & partners.
- **User Services** – driving exploitation by providing the right expertise and support to our users within a single synthetic environment.

Our services will be underpinned by a common technology architecture and externally recognised standards. This will accelerate delivery and enable multi-domain integration through the re-use of standard design patterns across Defence and with our closest allies.

¹This may be a distributed Cloud model to serve overseas deployed users and/or disadvantaged platforms.

²This includes “over-the-horizon” beyond line of sight deployed users and platforms.

How we will build the Digital Backbone

Defence's technology like many organisations has grown organically over time. To address our technical obsolescence and establish the Digital Backbone, we will build on the existing Core capabilities – the core technical building blocks of networks, gateways, hosting services, user interfaces (including identity management and access mechanisms) and middleware. We will also build on the investments we are already making to transform cyber security, rationalise our data centres, develop the next generation of networks and modernise our technology devices and supporting services.

Investment in Technology will deliver the multi-classification hyperscale cloud platform, next-generation resilient network, and modern user services that will come together to deliver data and information wherever and however we need to exploit it.

Above all, we will be delivering services that are intuitive, easy to use, reliable and secure.

Hyperscale Cloud for Defence

As a core building block, Cloud technology will provide the foundation on which we build and deliver the future capability we require. It is not a thing in itself but underpins and enables the advanced applications and services we need at speed, so we can keep pace with, and succeed against, our adversaries. It will enable and deliver on-demand services and applications that are easily accessible and rapidly-scalable; in turn, this will enable users to access and process data rapidly and securely on the battlefield, as well as enabling users in the business space to run systems, such as finance software, on the move.

Adopting new technologies – a 'growth mindset'

One of the ways in which we will keep the Digital backbone modern is to partner with the science & technology and research & development communities across Defence and with our partners and allies. Consistent with the MOD Science & Technology Strategy and R&D Delivery review, this will ensure that we search the breadth of S&T, make the right decisions and ensure that we break down the barriers to innovation and exploitation. Ensuring that industry can play a key role will be vital.

What this will deliver for Defence

By modernising our legacy estate and fully addressing our technical risks, Defence users will be working on robust, interoperable and cost-efficient technology infrastructure.

Hyperscale Cloud will be available at multiple classification levels providing the foundation on which new technology services can be rapidly built, adopted and scaled.

The next generation network will be in place, enabling military users to access and process data rapidly and securely on the battlefield, also providing friction-free data sharing with our allies and partners.

Security will be 'baked in' to our technology by design. New architecture standards and stringent governance processes will ensure that our technology remains future-proof, coherent and interoperable across Defence.

We will deliver efficiencies by bearing-down on single-use platform designs and rationalising the application-set, building solutions with re-use and portability at the heart.

Users will be supported by world-class digital and data services to enable them to rapidly exploit the value of emerging technologies to transform military and business outcomes.

Securing the Backbone



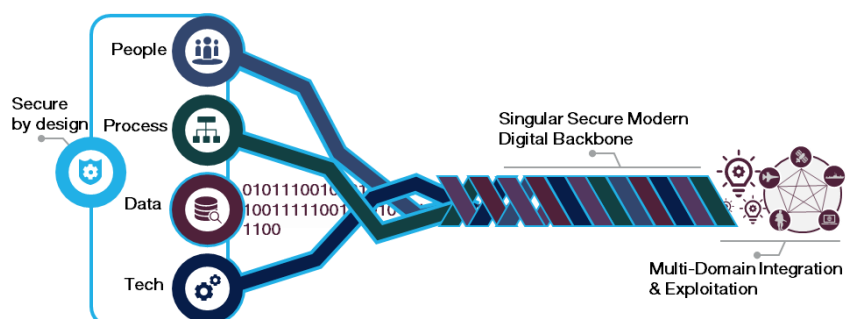
The UK has laid out its ambition to become a recognised global cyber power. To achieve this, it is critical that cyber risks are aggressively driven down to an acceptable level and that the Digital Backbone is secure by design.

Defence currently holds an unacceptable cyber risk position and faces an ever-rising wave of malicious cyber activity. The growing use of Digital capability in novel directions increases the MOD's cyber threat surface expanding the "active battleground" of cyberspace. In parallel, the proliferation of both state and non-state cyber actors who continually search for, and exploit vulnerabilities creates an imperative for action.

Extensive defensive cyber security gaps exist across the MOD in people, processes and technology; the Cyber Security Failure & Resilience risk is one of the top three Defence Board risks. MOD needs a rigorous approach to cyber defence where risk mitigation activities are driven aggressively, known vulnerabilities are addressed routinely, a positive cyber security culture is pervasive, and where critical and high risks systems and assets are made resilient to cyber-attack. This applies to all military and enterprise capabilities including the Digital Backbone.

What is needed to secure the Digital Backbone

The transformation of the digital enterprise will require the transformation of our approach to defensive cyber security. The UK has laid out its ambition to become a recognised global cyber power. To achieve this, a Secure Digital Backbone is critical. The Digital function has a lead role in aggressively driving down the cyber risk to an acceptable level while also driving cyber defence capability and modern crypt key into military and operational capabilities to ensure Defence tasks are delivered confidently in relation to the ever-changing cyber security threat. We will ensure the basics are done well and we have increasing confidence in the security of our information systems, networks, data and people.



“The rapid growth in demand for use of the electromagnetic spectrum (EMS), particularly as a bearer for cyber operations and a means of integrating domains and multiple partners, drives the requirement to compete more effectively for access and control of our networks; the resilient ‘train tracks’ along which our data flows. The ‘fight’ for the EMS is, and will continue to be, persistent and highly contested” - General Sir Patrick Sanders, Commander Strategic Command

How we will deliver the secure foundations to the Digital Backbone

- Improve the awareness and behaviours of our people to instil a positive cyber security culture across Defence.
- Modernise and transform the cryptographic solutions that keep our secrets secret.
- Instil secure by design as standard into the Digital Backbone and all capabilities across Defence based on modernised and simple cyber security policy and architecture standards.
- Develop the Identity and Access Management controls to enable the right people access to the right data and no more.
- Implement core security foundations to manage obsolescence, improve information management and ensure Defence has the right security tooling for its needs.
- Integrate the cyber defence measures to detect, respond to, and recover from a cyber attack.
- Identify, prioritise and remediate vulnerabilities in the current digital enterprise to minimise the Defence Board risk whilst transitioning to the Digital Backbone.
- Drive security improvements through the Defence supply chain.

We will deliver the secure foundations through three key programmes:

- Joint Crypt-Key Programme
- Defensive Cyber Operations Programme
- Cyber Resilience Programme

What this will deliver for Defence

By building cyber resilience in to the Digital Backbone we will have strong end-to-end Cyber Defence:

- ✓ Improved understanding of Defence cyber operating environment.
- ✓ Increased use of cyber capability to support planning and operations.
- ✓ Increased Defence cyber interoperability with national partners and allies.
- ✓ Improved Defence response to cyber threats.
- ✓ Increased Defence cyber resilience.
- ✓ Improved cyber culture across Defence workforce.
- ✓ Improved understanding of assets across digital Defence.
- ✓ Improved foundational cyber security.
- ✓ Improved protection of Defence against cyber threats.
- ✓ Increased Defence cyber resilience.

Automating support processes across the end-to-end supply chain

Deployed forces will be supplied via ‘intelligent pallets’ incorporating ‘sense and respond’ technology. The secure Digital Backbone will enable this deployed IoT capability to automatically update integrated inventory and transportation services and automatically resupply units according to the stocks consumed.

Strategic Command provides Defence’s Cyber Domain Leadership, and acts as the capability sponsor across the Cyber Domain. The Defence Digital Function, as part of Strategic Command, has a vital contribution in enabling and helping to protect the relationship and coherence between the operation and security of Defence Networks and the links to the broader capability areas, and offensive cyber.

Exploiting the Backbone

Effective exploitation of the digital backbone is critical for Defence to unleash the power of data and drive military and business advantage. The role of Defence Digital is to provide the core services and capabilities through the Digital Backbone, empowering the Commands and Functions to accelerate the digitalisation of Defence.

Opportunities for exploitation will be continually expanded and developed as the Digital Backbone is delivered. This section sets out some of the ways in which Defence Digital will support exploitation.

Battlespace and Functional collaboration – Customer at the Heart

Defence Digital will partner with the Front Line Commands, the Functions and their Digital Leaders to enable their transformations through Digital capability and shape their policies with Digital in mind. We will prioritise support for battlespace information capabilities, and promote the simplification, standardisation and automation of operational and support processes.

In support of wider Defence transformation we will collaborate with the Commands, Functions and other delivery bodies to shape the requirements-setting process for major services and change programmes, and define a more coherent digital demand signal for users.

Enabling rapid digital delivery through the Digital Foundry

We intend to enhance and expand our existing digital delivery teams to create a unique digital exploitation capability for all of Defence. Our vision is to establish a **Digital Foundry** in partnership with HMG and the best of British industry and academia.

The Foundry, which includes the AI Delivery Centre, will combine our new Centres of Expertise (CoEs) in Data, Automation and AI with new teams and skills. We will exploit the software-intensive capabilities that will give Defence a strategic edge in future military operations.

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-time¹. The Digital Foundry will follow proven agile delivery processes as set out in the government's Digital Service Standard & Service Manual.

The Foundry is a critical part of Defence Digital's strategy to exploit digital, data and technology across Defence.

Enabling autonomous Mine Counter Measure (MCM) capabilities

Route Survey Tasking and Analytics will deliver improved mission planning through digitisation of mission orders which can be accessed, reviewed and approved from any location, and enhanced analytics of maritime geospatial data to achieve best chance of mission success. The large volumes of high fidelity sonar data captured during MCM missions can be routed back to UK shores through secure data transfer at Secret via the Digital Backbone. This valuable data asset can then be stored and analysed as needed, including future Change Detection and R&D applications, providing information advantage and increased understanding of the global maritime environment.

Maximising the benefits of emerging technology

While we develop our vision for the Digital Foundry, we will continue to expand our Centres of Expertise (CoEs) for AI, Automation and Data to develop intuitive digital solutions on our multi-classification cloud hosting facilities. Our existing CoEs will continue to be the main vehicles for exploitation in the immediate future.

Exploiting our data

Defence's vision is that the effective capture, analysis and use of information at all security classifications will enable transformative benefits in the operational and business environments. We intend 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.

To drive data exploitation, we will:

- Cohere data demand across Defence, ensuring opportunities to optimise delivery are seized and achieved.

- Establish a world class analytics, data science and Artificial Intelligence capability and drive delivery of cross-cutting Advanced Analytics, Data Science and AI based projects.
- Collaborate with our international allies and National Security partners to drive operational and business value through data.
- Exploit game changing data technologies & capabilities for complex, joint or cross-cutting AI application areas and mission environments.
- Showcase and embed best practice data discovery and exploitation methods to deliver operationally-viable exploitation systems at scale.

Multi disciplinary delivery, working with industry and partners

We won't be doing this alone. To accelerate a fundamental shift towards data-driven and software-defined military capabilities, we will partner with DE&S, DSTL, industry, academia and our strategic suppliers. This ecosystem model will allow Defence to leverage the very best civilian technology and skills, whilst ensuring that our applications and algorithms are relevant, reliable and resilient, given the unique challenges we face.

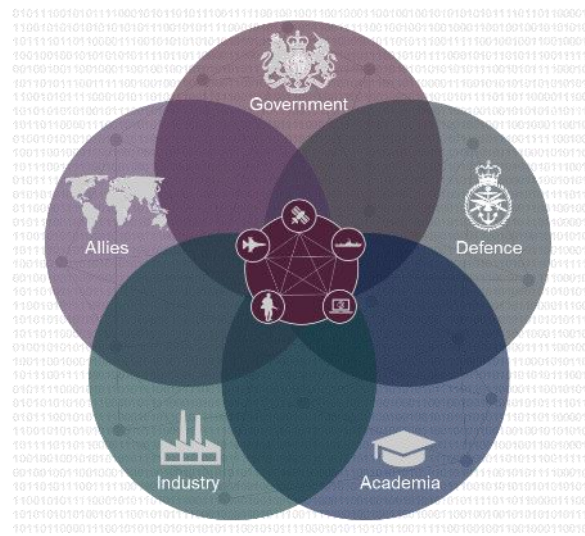
The Digital Foundry in action:



Integrating the Backbone

The ‘One Defence’ model is the only way for the UK to remain competitive in the rapidly-changing world of modern warfare.

Increasingly, we see military capability being combined with economic and diplomatic power to achieve desired outcomes. The future ‘Integrated Operating Concept’ for Defence will require seamless multi-domain integration and significantly increased partnering across government, allies, and with industry.



Historically, Defence has developed capabilities in organisational silos and often in isolation from one another. When procuring new systems, integration across the domains has often not been considered or has been traded out.

As a result, planning integrated operations is overly complex and we are not able to share, swap or integrate data at a speed that generates tempo and advantage.

In future, the core technical building blocks of the Digital Backbone; networks, gateways, hosting and middleware will together allow us to deliver data and information quickly and securely to wherever we need to exploit it.

The Digital Backbone will also provide the standard blueprint for integration, enabling our programmes and partners to design and build the friction-free movement of data across military and corporate domains – by design.

Through increased partnering and collaboration across government and with allies and industry, we will significantly increase our ability to leverage new, innovative, large-scale capabilities, whilst also lowering the individual financial burden on us.

Lastly, effective integrating mechanisms will bind Defence into a more unified enterprise which uses every technology capability in concert to support a desired outcome.

“We cannot afford any longer to operate in silos - we have to be integrated: with allies, across Government, as a national enterprise, but particularly across the military instrument” –

General Sir Nick Carter, Chief of the Defence Staff

Supporting collaboration across SDA and the nuclear enterprise

The Digital Backbone will enable us to collaborate with our allies and industry, at SECRET. We will work with them in real time, sharing data securely, quickly and easily; improving how we manage the nuclear enterprise



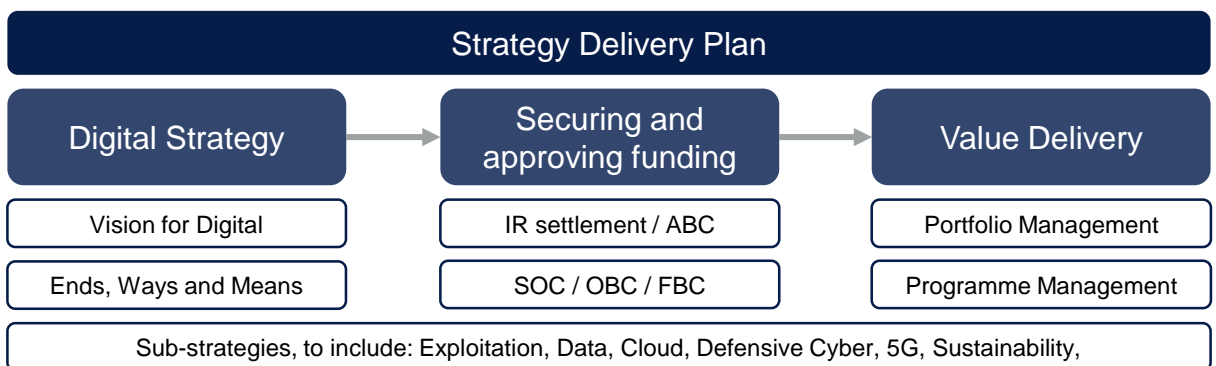
03 Means

Implementing the strategy

We will create early momentum by focusing on four key programmes – their combined outcomes will realise our objectives and create the Digital Backbone.



These programmes will turn this strategy into Digital outcomes through our Strategy Delivery Plan:



Dependencies

Implementation will have significant dependencies on other transformation activity, notably the parallel Functional programmes: People, Support, Acquisition, Culture & Empowerment.

Challenges

In order to deliver the Digital Backbone we must recognise and proactively address our constraints. These include securing multi-year investment, legacy commercial agreements, interoperability of existing platforms and our ability to influence some partner or industry solutions, as well as those of our allies.

Delivery



We will achieve our Objectives of building the Digital Backbone and accelerating adoption and exploitation through four Defence Plan Sub-tasks¹ – we will use our key programmes, along with a Functional Process ‘wrap’, to demonstrate progress and to hold ourselves to account:

15.1 Deliver Defence’s Digital Backbone

People – Drive the SQEP levels and mature Defence’s Whole Force Digital Workforce

- Adoption of coherent digital governance and digital skills frameworks

Process – ensure consistency, cohesion and integration across the Defence ICT estate

- Visibility of major ICT Investments
- Adoption of digital “rules of the Road”
- Financial efficiencies through IT Category Management

Data – Leverage data “as a strategic asset” enabling greater data exploitation

- Data Asset curation through Defence Data Strategy
- Data Risk Mitigation
- Adoption of Data “Rules of the Road”

Technology – Deliver the core technical digital and data building blocks

- Common technical Reference Architectures
- Adoption of Defence Cloud Services
- Rationalise Data Centres

15.2 Drive Effective Exploitation of the Digital Backbone

Enable Defence to exploit the data via the Digital Backbone to leverage modern digital WoWs across both Business and Battlespace

- All new data exploitation programmes to adopt a coherent approach utilising “Rules of the Road”
- Adopt pan-Defence Digital tools and services
- Institute Digital Boards to oversee agreed Digital Sub-strategies

15.3 Reset Cyber Defence

Drive cyber risk understanding and transform activity in order to drive down the intolerable cyber security risk

- Demonstrate progression in addressing Critical Vulnerability Gaps
- Produce Risk Mitigation Plans
- Embed “Secure by Design”
- Form a clear view of IT Obsolescence

Ensure sufficient SQEP cyber resource is available to deliver cyber risk reduction activity

- Embed Cyber security controls and risk mitigations as a priority into programmes and demonstrate compliance.

15.4 Deliver, Generate, Operate and Defend efficient and effective IT Capability

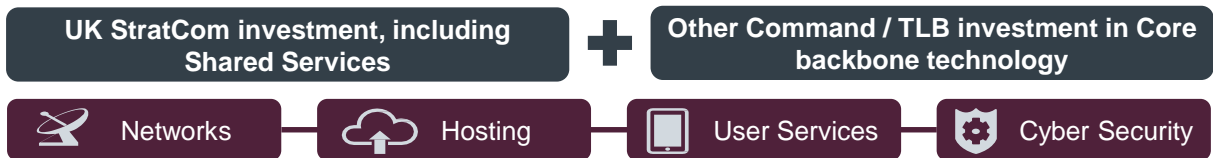
Plan reliable IT services that support operations, Plan and conduct Cyber Operations and Deliver the Digital Programme Portfolio

- Understand the Defence IT estate – a robust baseline of configuration data
- Strengthen Defensive Cyber and IT Operations with federated approach
- Coherent management and operation of Electromagnetic Spectrum capability
- Continue to improve Digital Programme delivery.

31 1. Defence Plan 21 Task 15 – Deliver Defence’s Digital Capabilities and Services that enable sustained military and business advantage and exploit Defence’s Data.

Investment and Benefit

There is significant programmed spend on Core Backbone technology over the next 10 years through the Equipment Programme – further investment will be made in building the singular, secure, modern digital backbone and unleashing the power of our Data.



Working with UK StratCom Cap as the primary sponsor area, and with Defence’s wider CIO community, we will continue to invest in core backbone technology, including shared services: network services, such as satellite network communications, tactical internet and communications, terrestrial network communications, and interoperability; hosting, such as applications and hosting services; user services in base IT, deployed IT, Above Secret and Integrated User Services; Cyber, such as cryptography and cyber security.

Additional investment required

To achieve the outcomes set out in this strategy however, and to build the singular, secure, modern Digital Backbone, there is a requirement for significant upfront investment in our priority programmes across People, Process, Data, Technology and Cyber programmes.

Financial Benefits

Digital Transformation will also enable and deliver financial benefits across Defence. At present, we are forecasting cashable and non-cashable financial benefits across four of our Programmes:



There is also significant indirect Financial Benefit (cashable and cost-avoidance) to be realised across Defence as Digital enables wider transformation across the Commands, Enabling Organisations and Functions:

- ✓ **Cloud:** savings on associated tooling and workforce.
- ✓ **Foundry ecosystem:** increasing mandatory use of common tools, vice local development
- ✓ **Automation:** releasing workforce into higher-value roles and improving MI
- ✓ **‘Sunrise’ software-defined capabilities:** reduced the requirement for legacy skillsets
- ✓ **Data:** cost-avoidance through coherence and reduction in mass duplication
- ✓ A smarter approach to Digital and IT suppliers across Defence.



Part 2

Operating Model

Digital Operating Model

The delivery of our strategy requires a strong, connected and cohesive Functional team working as a single entity across the federated Defence landscape. This section provides a summary of our Operating Model, with links to a more comprehensive set of documents

CIO Accountabilities

The Director General CIO is the principal advisor to the Defence Board on Digital and Information. CIO will provide Functional leadership to ensure Defence deploys and uses relevant, leading edge digital capability in support of Defence strategy realisation.

CIO will provide assurance that Defence is maximising value from its Digital investment and lead the function to establish Digital capabilities that will meet Defence's ambitions and needs.

CIO is held to account for the Digital Function through Permanent Secretary and the Defence Information Steering Committee, and for the Defence Digital HLB by Commander UK Strategic Command.

Maximise exploitation of Digital and IT

Deliver Effective and Efficient Digital and IT

Maintain a strong Cyber Defence

Maintain a strong Digital Function

CIO Authorities

The following Authorities and levers will ensure the strategic intent and accountabilities are met:

- ✓ To ensure TLB Digital sub-strategies and plans are consistent with the Functional Strategy.
- ✓ To set relevant policy and standards and ensure compliance including in all new builds.
- ✓ Tighten Data Controls and Authority: Formal governance across TLBs, Enabling Organisations through the DOM.
- ✓ Senior appointments: To be involved in the shaping of the role, the recruitment process and in approval of the appointment of senior SCS and military equivalent roles.
- ✓ Hold senior functional leaders to account for in-year delivery objectives in service of cohesion, integration, skills development and compliance.
- ✓ Set the standards and define the professional development goals and programmes to deliver skills.
- ✓ Drive a consistent and aligned approach through standardisation of CIO roles across Defence, delivered through accountability changes.
- ✓ To ensure cyber risks are effectively understood and mitigated.
- ✓ Making the pan-Defence ICT portfolio transparent and recorded / tracked using common processes and tooling.

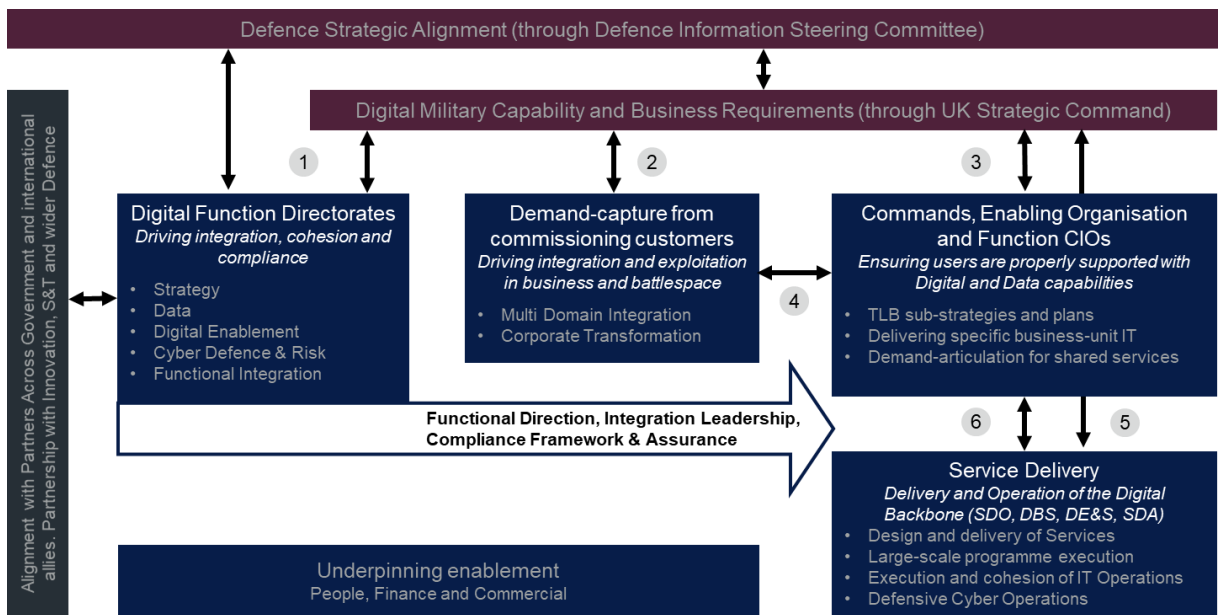
Our Operating Model has four key constructs:

Defence CIOs: Drive local sub strategies and plans; ensure that the business unit maximises benefit from the local and wider shared Defence investment in digital.

Demand-capture from commissioning customers: Leadership for the establishment of effective exploitation of the digital game-changers at scale in both military and business arenas.

Digital Function Directorates: Drive pan-Defence cohesion and integration; lead the creation and maintenance of the strategy and its execution.

Service Delivery: The engine room of programme delivery, shared service delivery, operations support and cyber operations.



Linking Processes and procedures

- 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.
- 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'.
- 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.

- 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.
- 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.
- 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).

Senior Leadership Accountabilities across the Operating Model

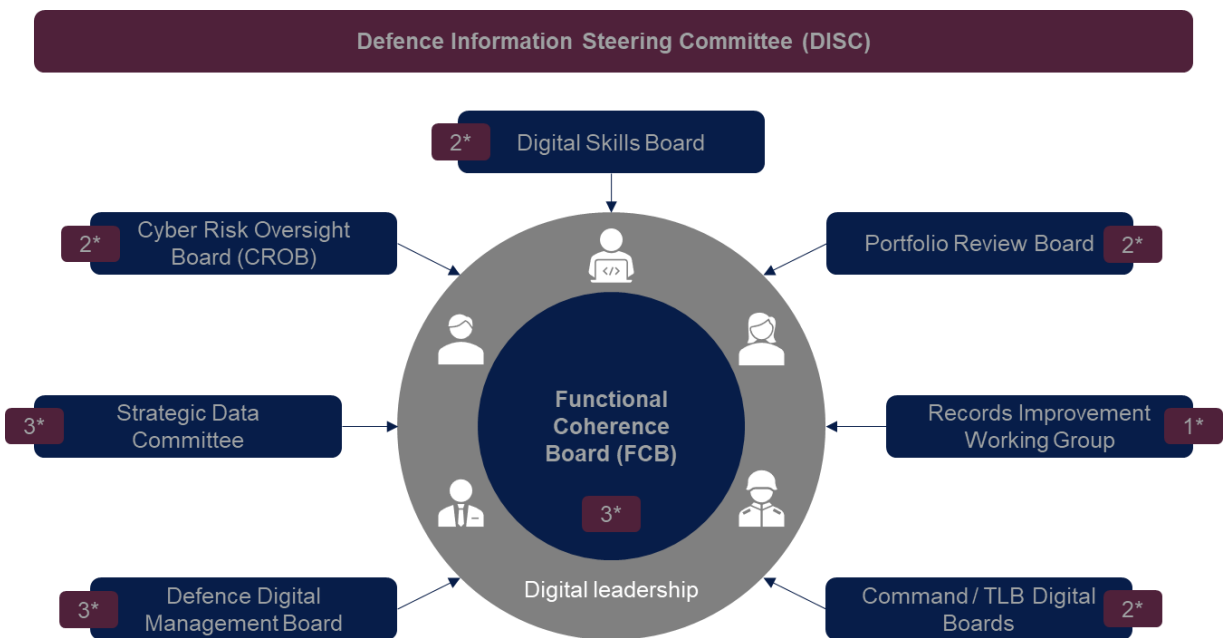
Defence CIOs	<p>CIOs for Commands, Enabling Organisations, Functions.</p> <ul style="list-style-type: none"> • Drive the Digital transformation of their organisation, underpinned by a 3-year digital sub-strategy; represent the voice of their organisation within the Function; contribute to the development of standards and processes. • As an integral part of the CIO's Functional Team, support the CIO driving forward Digital transformation under a single, transparent, pan-Defence ICT portfolio.
Digital Function Directorates	<p>Senior Leadership Team in Defence Digital, with pan-Function accountability</p> <ul style="list-style-type: none"> • Director Strategy: Engaging across Government, MOD, allies and industry to develop actionable Information and ICT strategy, driving transformation across the department. • Director Functional Integration: Ensures that the processes and mechanisms to manage the Function as a cohesive entity are in place and operated effectively. • Director Digital Enablement: Owns Enterprise Architecture and supporting technology and tooling frameworks; design and implementation of the technology backbone; evangelist for game-changing technology. • Chief Data Officer: Ensures a cohesive vision, strategy, framework and plan for the design and delivery of outcomes for Defence's access to, and use of, data as a strategic asset in service of sustainable military and business advantage. • Director Cyber Defence and Risk (CyDR): Defence lead for Cyber Defence and Digital & IT security; as CISO to provide leadership to ensure threats are understood and explicit risks identified and mitigated.
Exploitation Integration	<p>Senior Leadership Team in Defence Digital, with pan-Function accountability</p> <ul style="list-style-type: none"> • Director Military Digitisation and C4I Joint User: Work across military Commands to understand the end-to-end demand signal and ensure delivery is integrated across multiple domains. Work to UK StratCom Cap to profile the investment and ensure integration with the 'rules of the road'. • CIO of Functions: Prime interface with the main Defence Functions and business support / corporate service organisations to promote next-generation exploitation of digital and information technologies.
Service Delivery	<p>Delivery Organisations, including Defence's Digital shared services organisation</p> <ul style="list-style-type: none"> • Executive Director Service Delivery & Operations (SDO): Lead the delivery of shared Digital and IT user services, core infrastructure and IT Operations delivery, and ensure what is delivered is relevant to Defence needs. • Non-Digital Delivery Agents (Defence Business Services; Defence Equipment & Support; Submarine Delivery Agency): Deliver in accordance with Digital Portfolio Governance. Deliver TLB/FLC specific applications – that are built and supported according to the Function's architectures, standards and processes; and using the centrally provided tools and systems as part of a collaborative Digital portfolio.
Function Enablers	<p>Senior Leadership Team in Defence Digital</p> <ul style="list-style-type: none"> • Director Finance: Ensures that Finance is integral to decision-making and activity within Defence Digital and across the Function. • Director Commercial: Assertive management of suppliers and contracts, with a focus on IT costs and driving efficiency across Defence. • Deputy Director Human Resources: Ensuring that there is a workforce with the skills and capabilities needed, that is motivated to deliver and inclusive.

Governance

To deliver on our strategic vision for the Digital Function we have put in place a strong set of functional governance mechanisms to cohere planning, investment and operation of Defence's Digital Services and the data and information services they enable. Through a series of Defence and Function level boards, assurance is provided for the Function, along with forums for decision-making and escalations.

Defence and UK StratCom Boards. CIO is a member of the Executive Committee, Investment Approvals Committee, Joint Requirements Oversight Committee, the Transformation Board, Defence Operating Model Board, Defence Technology and Information Board and the Defence Delivery Group. Additionally, CIO has representation at the Multi-Domain Integration Change Programme Board, which is fed by the 2* Digitising the Battlespace Board.

Function Boards. Digital Function governance forums are in place to drive the Digital agenda of People, Processes, Data and Technology.



Function Boards

Digital Information Steering Committee (DISC): Sets the strategic direction for the Digital Function (Comprising: Perm Sec, Comd UKStratCom, VCDS, CIO, COO, DCDS MilCap, CRO plus the NEDs).

Functional Coherence Board (FCB): Act as the primary mechanism for TLB CIOs and Senior Digital Leadership to work collaboratively to mature the Digital Function.

Specialist Boards provide an important assurance function and provide inputs, decision-making, and escalation routes for FCB. Chaired by Defence Digital and wider Function leaders, these include Defence Digital HLB boards (and QPR), wider Function boards, and the TLB Digital Boards.

Policies, Rules, Guidance

Links to artefacts can be found on Defnet [here](#).

- **Policy** – including Defence Manual of ICT, Defence Manual of Security, Managing Information in Defence
- **Government Digital Service** – Manual, Code of Practice, Standard
- **Legislation**
- **Accreditation**
- **Defence Information Portal**

A link to the full Digital Operating Model on Sharepoint is [here](#).





Ministry of Defence