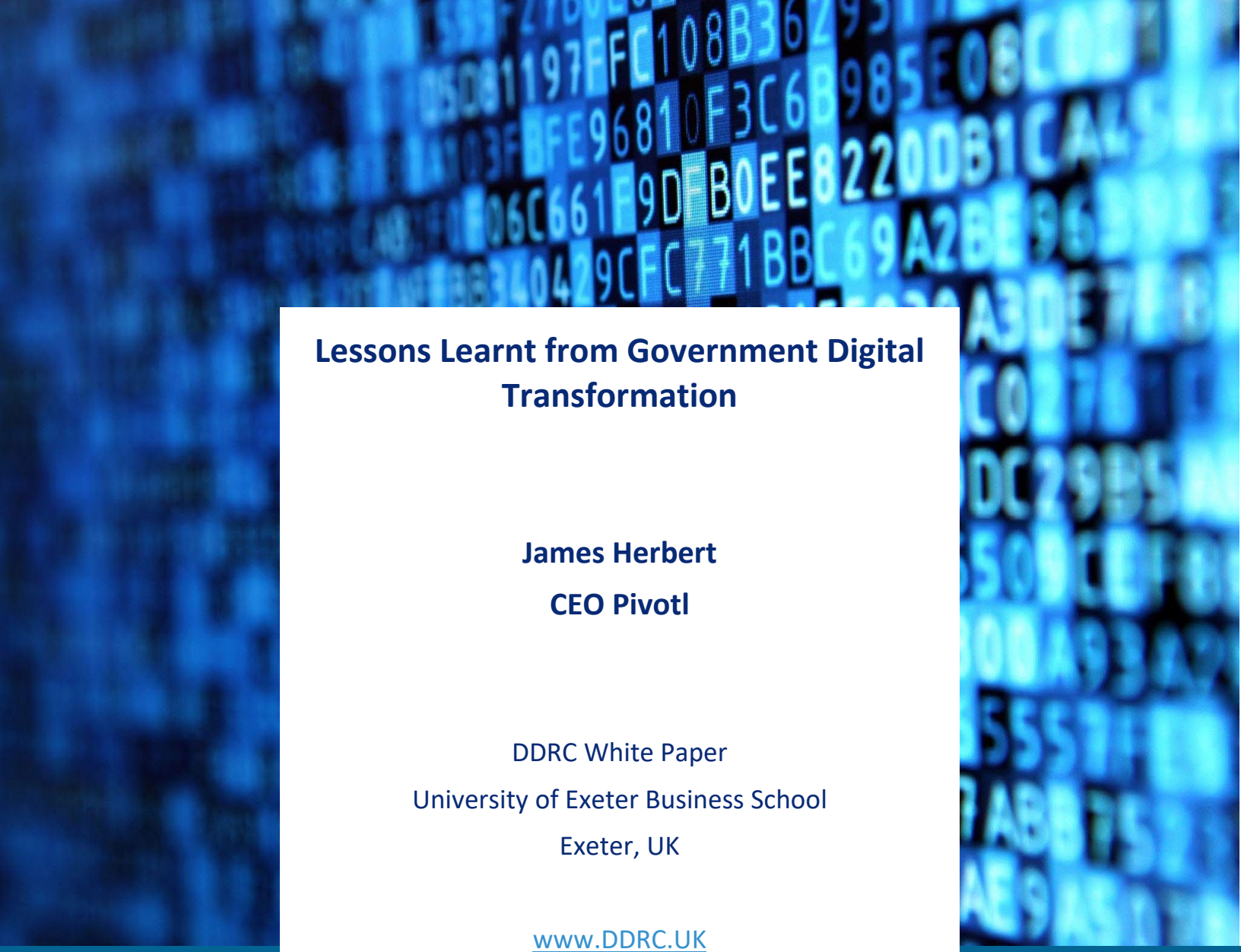


Lessons Learnt from Government Digital Transformation

James Herbert

CEO Pivotl

DDRC White Paper

University of Exeter Business School

Exeter, UK

www.DDRC.UK

July 2023

Report number: DDRC – 24/01

DEFENCE DATA RESEARCH CENTRE

Lessons Learnt from Government Digital Transformation

Executive summary

"A nation's ability to fight a modern war is as good as its technological ability."

Frank Whittle

Strategic Ambition

To meet the needs of modern warfare and to counter shifts in global geopolitical power, the UK Government (HMG) and the Ministry of Defence (the MoD) have recently published ambitious transformation strategies. HMG's vision for the future of UK defence embraces emerging technologies such as artificial intelligence (AI) and puts data at the heart of its approach.

In 2021 the MoD launched the **Digital Strategy for Defence** describing how its proposed transformation of technology, ways of working and processes will allow the seamless sharing and exploitation of data. The strategy recognises that data is a critical asset, but also that people and processes are as vital as technology to successful digital change. Successful implementation of the strategy will enable the UK Defence sector to operate more effectively in an era of disruptive technology and evolving security threats.

Similarly in 2022, the MoD unveiled its **Defence Artificial Intelligence Strategy**. The Secretary of State for Defence, Ben Wallace MP, at the time said that artificial intelligence "is one of the technologies essential to Defence modernisation." He said that the strategy would set out "how the MoD will adopt and exploit AI at pace and scale, transforming Defence into an 'AI ready' organisation and delivering cutting-edge capability."

There appears to be broad consensus across political and professional military lines that effective exploitation of artificial intelligence and data science will be crucial in developing a modern defence sector and in turn to securing the future prosperity and wellbeing of the UK.

"Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat."

Sun Tzu

The Right Tactics to Transform

Bold, transformational strategies only have meaning if and when they produce tangible positive outcomes - preferably at scale. In the last three years HMG has published thoughtful and well received strategic documents for Defence. But without the right tactics they will fail to deliver against their stated objectives. Or they may do so too slowly.

History suggests that the MoD faces an uphill struggle to deliver against the promise of its own strategies. The UK Government's track record in delivering complex, large scale technology enabled change is patchy at the best of times. When this transformation requires significant upheaval to working practice, culture and leadership style, success rates are even worse. The UK defence sector is large and complex with a significant legacy IT estate, large skills gaps and a limited supply base that is used to operating in a world that works at the cadence of hardware rather than software - all of this makes change challenging.

In fact, a recent House of **Commons Committee report** says the MoD has been struggling for years to deliver the major programmes necessary to replace over 2,000 systems and applications for its 200,000 users. These range from administrative and back-office IT to military platforms such as ships and satellites – with much of this on outdated legacy systems.

"The MoD as it currently operates is frankly not up to the task it faces," said Dame Meg Hillier MP, Chair of the Committee. "The scale and nature of the challenge of modern warfare is accelerating away from the Ministry, while it's bogged down in critical projects that are years delayed and at risk of being obsolescent on delivery. Two of its major digital transformation projects have been written off as 'unachievable' by the oversight body. There is no world in which that is an acceptable situation at the heart of our national defence."

The fact is, the MoD was late to the public sector digital transformation party.

The first iteration of the G Cloud framework was written in 2009, and the Government Digital Service (GDS) was established in 2011. Yet Defence Digital, the organisation charged with taking forward the UK's military digital ambitions was only formed in 2019, initially with a mere three members. This has since grown to more than 2500 members of staff and a budget of £2 billion but it's not clear how much of this is just the aggregation of existing IT capabilities and budgets from across the defence estate, and how much actually represents new

investment, new talent and new thinking. Defence Digital has just published its first Service Assessment Standards which is a hugely positive step but this is a long way behind the rest of central government agencies and departments.

Being late to the party matters, because digital transformation is an iterative process that builds upon individual and institutional learning. The goal is not to get everything right the first time around but rather to learn and adapt as experience and circumstances change. The final result is transformation caused by thousands of small changes and decisions, and it's hard to do this when you start so late.

However, UK Defence's late entrance to the party also represents an opportunity. While the wider public sector has certainly seen benefits from its digital transformation efforts there is much that hasn't worked or hasn't changed. This represents an opportunity for the MoD to learn from related experiences across government.

The Purpose of this White Paper

The paper is deliberately empirical in nature. The authors have spent 20 years working across multiple UK government digital transformation programmes - as officials, as consultants, as entrepreneurs, and as technologists - from high-level strategy work with the Cabinet Office through to scaled software engineering builds with DVLA and ONS.

The paper is not intended to be negative, but it has been written as a constructive provocation. The many successes of UK Government Digital Transformation are well documented, widely publicised and even copied around the world by other governments. There is little to be gained from repeating them here. But much remains unreformed and this fact tends to receive less airtime: tools and (Covid-enforced changes aside) working practices are largely the same as 20 years ago, data remains an underutilised asset, much of the workforce demographic remains stubbornly un digital and the sector consistently struggles to attract and retain the right modern talent needed for this sort of work.

This white paper explores the likely barriers to meaningful exploitation of AI and Data Science within the MoD based on the Digital Transformation experience of the wider public sector. The paper identifies five elements of digital transformation from which significant lessons can be learned:

- Procurement
- Technology
- Skills
- Appropriate Leadership
- Culture

The paper offers an overview of the experience of the wider (non-defence) public sector in delivering digital transformation programmes, pinpointing where Defence could learn valuable lessons. The crucial question must be asked: at a tactical level, what is it that UK Defence will do differently from other government digital transformation efforts to ensure success in Data Science and AI?

Section 1: Valuing Partnership and Ecosystems Over Procurement

The most successful software and data companies consciously position themselves as part of an ecosystem of suppliers, partners and talent. They either create and own their own platform which these entities can use to support their work, or they align with an existing platform, or number of platforms, upon which this can happen. This is because true success with data and software is hard for any single organisation to achieve on its own. Careful thought is needed about the wider ecosystem of people and partners that can contribute to the organisation's goals. Procurement forms part of this but it is only one aspect; partnership and access to an ecosystem are the real multipliers.

A 2023 report by the **Public Accounts Committee (PAC)** said that The Ministry of Defence must fundamentally change the way it operates to implement its new digital strategy at the necessary pace and scale. Yet it still does not have a delivery plan that will allow it to do this.

Much like other government organisations, Defence is struggling with a legacy IT estate, an explosion of siloed, unstructured data and a lack of interoperability between systems. However, if you talk to anyone in and around Defence, they will usually say the greatest barrier to change is procurement and commercial management. On this, lessons can be learnt from the evolution of government technology procurement over the past 15 years.

Pre-G Cloud Technology Procurement

Government historically sourced technology services and products from a very small group of global outsourcers and consultancies via lengthy and costly procurement processes. Only large companies could afford to take part, so over time this created an 'oligopoly' of Government IT suppliers. An oligopolist supply base can be just as limiting and neophobic as a monopoly – particularly if the parties all act in the same way and benefit from similar commercial models - and this arrangement certainly did not encourage partnership. Relationships were contractually focused with high penalties for deviating from pre-agreed specifications, bounded by aggressive change control and price sensitivity. These procurement processes also didn't open public sector organisations up to a wider ecosystem of ideas and approaches. In fact, such locked down arrangements actively discouraged the development of broader supply chains for government organisations.

In the mid-noughties the emergence of a new technology paradigm, that of public cloud, meant that these costly and restrictive arrangements became increasingly unfit for purpose. The early promise of public cloud and agile software development practice was iteration, experimentation, agility and a pay as you go

commercial model. None of these features were in the best interest of the Oligopoly. Their commercial survival required long term, rigid contracts allowing them to charge even for minor changes. There was little incentive to surrender their grip on procurement in government.

At the same time, the government's approach to procurement was set up to facilitate the Oligopoly's success – large, lengthy and onerous point procurements or a limited number of frameworks underpinned with requirements only achievable to the largest of companies.

The Coalition Government, elected in 2010, decided that something needed to change as a matter of official policy. That change was delivered initially in the form of the G Cloud procurement framework.

G Cloud Enabled Partnership and the Potential of an Ecosystem

The original goal of the G Cloud Framework was to make bidding for government projects cheaper, more collaborative and more transparent. It restricted the duration of contracts to an initial two year period and allowed for greater transparency over who was spending what and with which supplier. But the framework's more strategic goal was to open the public sector up to partnership with more innovative suppliers and to an ecosystem of different specialists. It was attractive to smaller companies for several reasons:

- G Cloud slashed the cost of entry to government contracts for SME suppliers. In the five years following its launch, it hosted thousands of suppliers offering different types of products and services.
- It also enabled the big cloud providers to sell their platforms to government agencies, upon which SMEs could innovate and build services.
- It allowed a buyer, when faced with a problem to solve, to quickly shortlist a small number of suppliers and start talking to them before a procurement was even published. In other words, the supplier could understand the client's problem from the start. When the time came for a proposal, the supplier therefore understood the job in hand, the skills that would be required and whether or not the technologies they specialised in were relevant. Generally, a more informed, collaborative procurement process such as this leads to better outcomes for both the client and the supplier, and ultimately the taxpayer too.
- The two year (plus 1) contractual commitment allowed suppliers to invest in the work and the client without locking the government body into onerous lengthy contracts.

Flaws of G Cloud

The G Cloud was an undeniably crude approach with some clear flaws. The lack of standards required to list on the framework meant that buyers were not necessarily nudged into making better technology decisions, just faster ones. This lack of control also meant that many recruitment businesses were able to list on the platform. For some buyers it became a quick way of sourcing 'bodies' rather than building an ecosystem of strategic technology partners. Finally, the need to balance openness with ensuring procurement decisions weren't based on relationships and other non-core factors was never really resolved.

From around 2015 onwards the government procurement profession moved to mitigate these issues. In 2016 the UK was ranked number one in the United Nations E-Government Development Index (EGDI). By 2022 it was ranked 11th. There are multiple reasons for this but it's likely that one of them was the dilution of the early benefits of the G Cloud.

G Cloud's Decline: Separation of Expertise from Technology

In an effort to prevent the use of G Cloud as a disguised recruitment framework, the Crown Commercial Service (CCS) brought in the **Digital Outcomes and Specialists (DOS) framework**. G Cloud is for SaaS and cloud-based products, and DOS is for digital people and teams. DOS has thousands of suppliers listed on it and the barrier to entry is low. Despite this, it is not a sophisticated enabler of partnership and ecosystems.

Via DOS, government buyers publish large numbers of requirements to the entire market. The quality of requirements is patchy and of varying detail and quality, plus there is no formal mechanism for the supplier community to understand more about the buyers' needs so they guess what they think the buyer wants to see. The responses received are almost entirely case study based, so over time this means organisations that already do a lot of work with government win more work.

This reduces the sector's exposure to new suppliers and a form of new, medium sized 'DOS Oligopoly' emerged – companies that are best at answering DOS questions rather than necessarily the most innovative or effective win. Often the successful supplier turns up on day one with a team that is not relevant for the work as the buyer has not accurately described their need and there has been little pre award opportunity for developing shared understanding and collaboration. Feedback to suppliers that didn't win is perfunctory and lacking in detail which limits the ability of the market to build general understanding of the needs of government.

Outsourcing to 'Premium Body Shops'

As part of its digital strategy the government rightly abandoned the use of inflexible 10-year, outcomes-based contracts for something more agile, flexible and within their control. But what they often end up doing in practice is using smaller suppliers as 'premium body shops' - over time that has replaced traditional IT outsourcing. Requirements are issued from that perspective, and it's common to hear requests like: "Give me four developers, a business analyst and a product manager."

For suppliers who know how to 'play the DOS system' this can be a reliable and profitable revenue stream, but there is little opportunity for organisations to engage strategically and shape the sector's approach. The most successful software and data companies consciously sit at the heart of an ecosystem of talent and partners. If

the Government's ecosystem is two hyperscale cloud providers and a small number of medium sized premium body shops, then the point of reforming procurement in the first place has been missed.

Compliance over Outcome

Despite this dilution in the original goals of the G Cloud, the Government has retained its commitment to spending a certain amount of public money (£1 in every £3) with SMEs. However, when it comes to technology procurement, larger public bodies are increasingly meeting this obligation by making SMEs work through large suppliers.

This happens as follows: the buyer runs a procurement, awards the contract to a large supplier - often a member of the original Oligopoly - but contractually binds the winner to spend a percentage of the contract revenue with SMEs. Financially, that means an SME can indeed make money from government projects. But they are often removed from direct contact with the client and become a body shop to the primary contractor. So, if the idea is to engage with SMEs in order to access innovation, a wider experience base and to bring different products and services to the table, it fails.

The Defence Buying Context

"The Defense world…was repeatedly ambushed by many of the technological disruptions flowing out of Silicon Valley. It missed the commercial space revolution. It missed the move to Cloud Computing. It missed the advent of modern software development. It missed the centrality of data. And it missed the rise of artificial intelligence and machine learning."

Christian Bose, The Kill Chain.

When it comes to purchasing technology, defence is in a similar place to where the rest of government was 10 years ago. It too has longstanding relationships with a particular group of suppliers and has traditionally been bound by the same strict structure and guidelines. This concentration of the supply base has become more acute over the last 15 years during which time there has been a significant amount of corporate consolidation. A decade ago, there was more depth and variety of defence suppliers to the UK and the US defence sector, but cuts in defence spending have forced markets to contract and consolidate.

It's not easy for companies to work with the defence sector. Of all the many tech focused Unicorn businesses created in the last 20 years only two - Palantir and SpaceX - chose to base their business model on the defence sector. They did this partly because they each had billionaire owners willing to stay the course with an almost unlimited chequebook.

Additionally, the DNA of traditional defence contractors is building large scale platforms such as aircraft, tanks, and missile systems. These platforms are essential and will continue to be needed. However, the heritage of the companies that build them is not iterative, agile, integrated and data driven - they are experts at hardware in a world where it is software that differentiates. To exploit AI and put data at its heart, the UK Defence sector therefore cannot rely on these contractors and the 'Premium Body Shopping' approach we explored earlier.

To add some more industry context, in 2022 alone, Alphabet, Apple, Amazon, Meta and Microsoft spent a combined $223 billion on R&D. Roughly 10% of their combined workforces'. LinkedIn profiles suggest they work in AI; they are making roughly one investment a month in AI specialists; and since 2019, a fifth of their combined acquisitions and investment were in AI. In fact, Microsoft alone has already invested circa £11 billion in OpenAI.

UK Defence doesn't need to be Microsoft or Apple, and indeed it shouldn't try to be. But it does need access to as broad a base of relevant partners and talent as possible. To achieve this is not a procurement question but rather one of strategic supply chain, partnership and platform thinking. A revised, modern procurement approach can then support delivery.

Recommended Takeaways

Defence has an opportunity to learn from some of the successes and mistakes of the past, particularly those of G Cloud and DOS.

The UK Defence Sector should develop an ecosystem and partnership approach. The features of which should be directly linked to the objectives of the Digital Strategy for Defence and The Defence Artificial Intelligence Strategy. The Strategy and associated plan should be shaped by broader, global trends in technology, data and AI and the implications of those trends for the sector. It shouldn't be based on historic or current buying practice. Among other features the strategy should:

- Outline what will be needed from the wider marketplace in order to achieve UK Defence's strategic objectives.
- Publish technology and data standards for the marketplace to work to and bake them into a procurement process.
- Consider a defence platform economy. What might that look like - in this context how do both the buyer and supplier sides operate to garner the benefits of a platform effect?
- Review the role of SMEs - clarify why they are important to defence and what they bring that cannot be found elsewhere. From this build out a commercial approach that encourages relevant SMEs to bid for work in defence because they bring something that the sector needs. Reconsider making them work through larger suppliers.

- Develop a commercial approach that supports all of the above - this could include using existing frameworks to access the market but with specific guide rails setting out which route is appropriate for which type of buying activity.
- Include a specific approach for how to deal with the hyperscale providers - being overt about the right way of managing lock in, security and costs.

Section 2: From a Project to a Product Mindset

"Another flaw in the human character is that everybody wants to build and nobody wants to do maintenance."

Kurt Vonnegut

UK Government Digital Success

GDS transformed technology-enabled project delivery across UK government services. Their focus on establishing the user need, technology principles, spend control, agile methods and service standards brought about a permanent sea change in why and how online public services are delivered. For redesigning existing digital public services or launching new ones, GDS' approach represented a genuine step change from what had gone before.

GDS has been copied around the world. Ministerial acclaim, OBEs, awards, books and new businesses followed on the heels of this genuinely significant achievement. Now, on the back of this refreshing thinking sits the promising recent work of the Defence Digital team.

However, whilst it's sensible for Defence to emulate the best of public sector digital work that has come before, the sector should be just as conscious of what hasn't changed, despite a decade of strategies, goals and promises. Redesigning a number of digital services based on user research and an iterative development method will contribute positively to the UK defence sector. But scaled exploitation of AI and data science requires much, much more. To complicate things further, those digital projects can be a distraction from grappling with the more fundamental challenges faced by a large, complex and longstanding organisation seeking to exploit data.

What Was Left Untransformed

Even with the advent of GDS, the UK's digital government approach did not evolve to truly transform how technology and data is organised, funded and looked after within public bodies. As digital delivery was devolved from GDS out to departments and agencies, enforcement of technology decisions and standards became more fragmented and less well governed. Spend control was loosened and while the need to 're-use' technology and service patterns is an often-quoted mantra, its practical application is patchy.

Increasingly, the government digital transformation landscape has become a place to either redesign or build new online services to execute straightforward transactions between government and citizens. Despite billions of pounds spent on digital in the last ten years, data is still siloed, underused and often of questionable integrity. Few major legacy systems have been switched off and the day to day technology experience of many civil servants remains poor.

Behind the scenes, legacy technology, legacy practice, legacy suppliers and legacy thinking predominate. Leadership across the public sector still views technology investment as a one off, temporary event - a project. When the project is delivered the system is passed to an external support service or IT; this then becomes business as usual and attention turns to the next new, capital-funded digital service build. Within this workflow the ongoing management, maintenance and development of even large scale, complex and high performance systems can appear to be an afterthought.

The opportunities provided by the smart implementation of a 'devops' culture and working practice - such as increased speed of delivery, fewer bugs, enhanced security, scalability, reliability - are rarely considered beyond the initial project of Discovery, Alpha and Beta.

Reluctance to grapple with the ongoing development, integration and testing of technology is understandable. To move from a project mindset to that of a product and Devops culture requires significant change to governance, working practices, culture and financial processes. Leadership must have some understanding of why this is a good thing and explicitly enable and support its implementation.

In other words, for complex, long-standing institutions it's not easy and not without risk. The problem is that to exploit data to the degree outlined in HMG's defence strategies this level of change will be required.

Technology and High Performance Organisations

The most successful companies in the world see technology and software as the permanent key enablers of their services and performance. For them, technology requires ongoing investment, appropriate supporting, organisational design and an understanding that there is never a point when any of this is finished - in other words, they think of technology as a product. It is the focus of a permanent team of specialists who keep developing, iterating, testing, and innovating it, capturing user feedback loops to improve experience and performance.

With both the presence of tech savvy leadership and a lack of legacy IT, these modern businesses have been able to develop a platform engineering approach to deliver high performance software at scale. By standardising infrastructure, using automation and building self service interfaces for developers, they have been able to build, ship and operate applications more quickly, securely and at higher quality. Crucially, the model works because there are dedicated teams maintaining all of this with appropriate budgets, working practices and tooling.

Since the platform itself is treated as a product - not the legacy of a previous project - the team needs to have development, operations, product management and product marketing skills. Ongoing product development is driven by collaborative learning cycles between the team and the platform's users, rather than by top-down mandates. This approach reduces friction for developers who can sit nearer to the customer in multidisciplinary product teams while allowing the organisation to retain control of technology choices, data standards and spend.

Why Does This Matter for UK Defence's Data Goals?

The Limitations of Existing Government Digital Transformation Paradigm - Defence is correct to adopt and learn from the frameworks and methods espoused by the last 10 years of government digital transformation initiatives. However, it should be equally conscious that there is much that has not been reformed or modernised. Doing only the same things and expecting a different result would be unwise.

Platform Engineering - HMG's data and AI vision cannot be achieved without excellence in infrastructure and software. Data and their related opportunities reside in those entities - a more sophisticated approach to where technology sits, increased investment levels and significant organisational change will be needed for the scaled exploitation of data.

Data Architectures - it is likely that defence will need to develop a similar model for data to that of platform engineering. Since the defence sector is so large, fragmented and complex, it may have to consider some version of 'data mesh' architecture - whereby a central data platform team provides core data capabilities that can be reused by all the other teams to self-serve their data needs. This will allow a platform to scale in a cost-

effective manner to meet the growing data demands of the defence sector and to meet government strategy. This would be easier to bring about with an existing platform engineering model in place.

The Role of Suppliers

When faced with complex and seemingly intractable technology problems, it is tempting to turn to the market for answers. Clearly, the MoD will need to work with partners extensively to realise its data vision. However, the thinking and design behind the problem of how to look after technology as a product rather than a project cannot be outsourced.

The nature of potential partners should be considered very carefully too. Many SMEs with a bias towards government digital transformation work lack real world experience of running live production systems. They are often design-focused, specialising in the front-end web applications or lightweight business applications for activities such as case management.

The big outsourcers can look after technology in the traditional support sense and they have the process infrastructure to operate in a business critical, secure environment. But they have certainly not been pioneers in the field of product mindset and platform engineering and cannot be relied on to innovate on behalf of their clients.

Key Takeaways

Defence should develop its own approach to adopting a product mindset. This should be pulled together by a multidisciplinary team drawn from DDAT, HR, finance, industry, academics and user representatives (the military). The team should arrange a study visit(s) to established organisations that have successfully implemented a platform engineering model and culture, in order to learn how to apply this to their context.

Among other topics the approach will explore and establish:

- Data and technology standards and enforcement measures,
- A platform engineering model for defence,
- A data platform engineering model for Defence covering,
- Data governance and data quality tooling,
- Self-service ETL and ETL data pipeline capabilities,
- Tooling and infrastructure to provide and/or support for data transformation, aggregation, segmentation and machine learning,
- Data visualisation capabilities,

- Metrics layer capabilities,
- Data storage capabilities,
- Clarification of the role of suppliers - what are their responsibilities versus those of the MoD?
- Investment profile.
- A review of supplier management in this domain. SME specialised consultants with experience of building and running products, who know public cloud platforms intimately, very rarely get an opportunity to share their knowledge directly with government clients as contracts are commonly awarded to big consultancies and systems integrators. So once again, there is some value to be found in engaging with people and organisations that are cloud native, and have a cloud engineering skill set, as well as the traditional, large suppliers.

Section 3: How Do You Build An Appropriate Skill Base?

"The MoD does not have enough people with the right digital skills, which is affecting delivery of the strategy. It finds it hard to recruit and retain talent because it cannot match private sector pay, and because the pay scales available to digital specialists in government vary. Technologists see the MoD as bureaucratic and the hiring process – including getting security clearance – as too lengthy. The shortfall of technical skills is affecting the delivery of both individual programmes and the strategy." – **National Audit Office: The Digital Strategy for Defence: A review of early implementation, October 2022**

The Digital Skills Gap in the Wider Public Sector

According to a report conducted by **Global Government Forum**, half of those working on digital transformation projects in the public sector say they struggle to hire qualified talent. This means that even when transformation projects are approved and financed, government bodies lack employees with the skills to implement and maintain these systems. The research shows that nearly all civil servants believe technology is key to unlocking public sector transformation and are committed to innovating the way services are delivered. But only six out of ten believe they have intermediate, advanced or highly-specialised skills and knowledge of how technology and data can transform services. From empirical observation this six out of ten self-assessed score is likely to be on the generous side.

Although most people are familiar with the concept of the digital skills gap, at a macro level it can appear to be a somewhat abstract concept. Nevertheless, in terms of using digital approaches and technology to reform public service delivery, it has had very real implications:

- **Over-reliance on suppliers and premium body shopping** - Digital projects are staffed and often even led by specialists from suppliers. Generally, there are a small number of civil servants that embed into these supplier dominated teams. While these civil servants are often highly capable generalists, they rarely have significant technical experience of the role into which they have been drafted. This increases the costs of change and leaves the government body unhealthily reliant on suppliers.

- **Lack of deep technology skills** - GDS made good progress in the establishment, development and description of the key digital professions needed to deliver digital transformation. Within some digital roles - particularly those of design, delivery management and user research - there has been a significant increase in permanent civil servant headcount, however there are still very few permanent modern cloud and software engineers. These skills are at the heart of modern digital businesses - a lack of them weakens the resilience and institutional knowledge of the government body.

- **Product ownership** - this is a crucial role in any digital, software enabled initiative and it cannot be ignored. The product owner is an expert in the service area undergoing transformation. They develop and communicate the product goal as well as prioritising the work. It is common for a government organisation to not assign a product owner at all to a digital build or to ask the supplier to do it for them which is suboptimal. Even more frequently they appoint someone who doesn't understand the role and doesn't have the bandwidth to focus on the work. This means the redesign and rebuild of products and services is not driven by someone that understands the business area and work is not prioritised according to greatest need.

- **Churn of senior leaders with experience in digital** - most leaders in government with significant digital experience join as contractors or become contractors after a period operating as a permanent civil servant. They move from transformation programme to programme fairly rapidly, rarely seeing an entire programme through which reduces their level of full life cycle expertise and causes disruption to the programme they are leaving. Even when contractors are not used, given that the average tenure of a senior civil servant is less than two years, this is not long enough to see through a complex technology enabled transformation and incurs greater cost in terms of recruitment and backfilling.

- **Lack of strategic HR involvement** - For many years the talent needs of digital transformation programmes appeared entirely untethered from the HR policies and approaches of the departments within which the work was taking place. Approaches to recruitment, retention, pay grading, job evaluation, career development and organisational design almost appear to have been designed to make building a digital workforce as difficult as possible. There are improvements being implemented now such as ring-fencing digital roles from the core job evaluation scheme but change is slow and incremental. Vacancies, lengthy time to hire and churn contribute to greater costs and lower quality delivery.

The Data Skills Gap

Obtaining, retaining and growing the talent required to ensure the MoD can 'adopt and exploit AI at pace and scale, transforming defence into an 'AI ready' organisation and delivering cutting-edge capability' is likely to require even greater thought and effort than previous attempts at securing digital skills.

Rebuilding services in a digital way can, to some extent, be carried out to the side of an organisation in a programme structure using large amounts of external resources. But exploitation of data to the level desired in UK defence requires the entire workforce to become data literate - from the executive leadership team to the front line. The technical data roles required for such a change are more varied and technical ranging, from visualisation specialists to full stack data engineers, through to PHD-educated data scientists. This is not a problem that will be confined to defence or the public sector.

In a large-scale World Economic Forum research study from 2019, it was found that only about 32% of executives felt confident in their skills to use data and, again, as with many self-scoring surveys this is likely to be generous. So, in many cases, executive teams are setting a data strategy when only one in three of them are confident in the use of data.

The younger workforce fares no better. In the same study it was found that in the group aged 16 to 24, only 21% were confident in their data literacy skills. It would be a mistake to assume that a generation raised by the internet, social media and smartphones is somehow inherently more capable of exploiting data and analytics.

The Democratisation of Data

Data is at its most powerful when the unique talents, abilities and experiences of an organisation's workforce are able to use it and make decisions based on it. Only then can the investments that have been made in software, data and technology be realised. Huge modern software companies have grown up over the last two decades offering the opportunity of democratising data to their masses. However, although products such as Tableau, Qlik and PowerBI are useful, when they are rolled out to an inadequately prepared workforce they actually make the data skills gap more acute. A 2019 survey showed that when workers without a technology or data background are asked to take on new software to exploit data, more than half of them would try to avoid using it.

To be clear, the democratisation of data is essential for UK Defence to achieve its modernising strategies and is a relevant goal. But a software and product led approach that doesn't address non-technical constraints will fail to deliver against HMG's Defence Strategies. It is easier to buy a software product than it is to educate an entire workforce - the temptation of the easier path should be avoided. Technology choices and plans should be realistically set against the capability of the workforce.

Skills Gaps in Defence

Defence is affected by digital and data skills gaps just like most other sectors. “The MoD faces ongoing challenges with its implementation of major technology programmes and acquiring scarce digital skills,” said Gareth Davies, head of the National Audit Office (NAO) in a **2022 report**. “The MoD needs a clear plan for prioritising resources to where they are needed most urgently if it is to deliver its ambitions for digital transformation.”

The skills base is particularly low when it comes to AI. A third of those surveyed in the previously referenced Government Forum survey said they have very few or no skills or knowledge in how AI and automation can be used to improve public services, with only 5% having received any training in the technology. Fewer than a quarter of civil servants agree that their department has the necessary skills and expertise in AI or machine learning. We can assume the numbers may be similar in the Defence sector.

Culture Versus Pay

Many civil servants’ pay is aligned to how their job is graded. Much of the weighting of the grade is based on the size of their budget and the number of people that they manage. But this hierarchical approach is at odds with hiring AI and data science professionals. It could be that there is an AI specialist, with a PhD, who has incredible experience in other sectors that they could bring to defence. To get the best out of their talent it might be that they manage no one and do not own a budget. But an historic job evaluation process won’t allow the hiring organisation to compete on salaries in the marketplace.

Competitive pay and rewards are important and can require some significant changes to an organisation’s overall people model. But in the digital and data space, culture, working practice and tooling are equally important considerations. Even the most public spirited engineer, AI specialist or data scientist will get frustrated by overly onerous bureaucracy; by the fact they can’t hire the teams they need because of hierarchical structures; or because they find that leaders are just paying lip service to a project as they don’t really understand it.

So even if Defence can offer more competitive packages to attract data specialists, these people won’t last long in the sector if they are faced with insurmountable bureaucracy, or just get burnt out by the lack of wider organisational understanding of what they’re doing.

Key Takeaways

The UK Defence Sector should develop a talent and people approach, the features of which should be directly linked to the objectives of the Digital Strategy for Defence and The Defence Artificial Intelligence Strategy. The Strategy and associated plan should be shaped by broader, global hiring trends in technology, data and AI and the implications of those trends for the sector. It shouldn't be based on historic or current Human Resources practice.

Among other features the approach should:

- Be developed by DDaT specialists in conjunction with relevant HR teams and representatives of relevant suppliers.
- Be realistic about the data skills gap. How far is it possible to close the gap and at what speed? How can talent constraints be mitigated? What measures should be developed to monitor the appropriate balance between in house and external resources?
- Be aligned with technology choices. To what degree can automation and low code development platforms allow the defence sector and their staff to design, develop, deploy and run applications more effectively and efficiently? Might they allow users to access data and even build services on top, without relying on external suppliers?
- Be research and data led. What attracts the relevant talent to other organisations, both in the public and private sector? This should focus not just on attraction but filter down to a practical level to understand what keeps the talent working there. How can Defence incorporate these aspects into their working practice?
- Be mindful of the importance of executives (including military) in advocating for, and consistently reinforcing the criticality of software, data, AI and data science professionals to the future of the sector.
- Be brave in understanding and challenging historic HR practice. Speak with HR about its job evaluation framework to try to identify any solutions to the issues around pay weighting.
- Be confident and positive. There are many people who are genuinely motivated by working on technology projects that have inherent societal value, rather than just financial gain. How can that purpose be marketed? What innovative solutions could there be, such as relationships with universities, and a 'Teach First' approach for graduate technical and data specialists?
- Contain an approach and plan for training the entire workforce in data literacy. Leaders, in particular need to learn about data but also about their role in enabling data led transformation to happen.

Ultimately, the fields of data science and AI are highly technically complex, and therefore require corresponding intellect and credentials in their talent. Defence should therefore be honest with itself about what talent it can attract to build and run AI and data science programmes at scale.

Where hurdles are unlikely to be overcome, there needs to be an acceptance of dependence on external suppliers. The approach to this should be aligned with the Ecosystem and Partnership Approach detailed earlier in this paper.

Section 4: Leadership strategy and management

"We are in a leadership crisis. We are not in a technology crisis."

Marc Benioff, CEO Salesforce.com

Genuine, organisation-wide digital transformation is hard. Becoming truly digital, and truly data driven requires fundamental changes to culture, ways of working, business models, finance process, people process, governance, measurement, structure and value chain management. These changes can't be confined to a specialist DDaT team that sits to the side of an organisation. Everyone has to feel and be part of the change.

To lead through this undertaking would be a daunting task for anyone. But for those that have to contend with politics, treasury constraints, unions, PACs, inflexible HR frameworks, extreme talent shortages, procurement bureaucracy, media scrutiny, legacy technology and ever-changing ministerial strategies, the task must feel overwhelming.

Despite these challenges, it is the job of the most senior leadership in the public sector to ensure that its various services are fit for the modern world in which we live. Throughout the past ten years there has often been a stark gap between the digital strategies that senior civil servants publish and promote and their own practical efforts in enabling them to happen. Their published strategies describe the 'state of the art' while paying scant heed to the 'state of the practice' within their organisation. This begs the question - if the top level of leadership won't make the changes that need to happen to allow their own strategy to succeed, then why would anyone else?

The Leadership Gap

So, as well as a skills gap there is also a leadership gap.

In late **2022, EY reported** that only seven percent of surveyed government leaders said their organisation had achieved its digital transformation objectives. The findings are a damning reflection of digital leadership in government, demonstrating:

- A lack of digitally-aware leaders who can reimagine the citizen experience and change the transformation plan.
- Workforce actions that are reactive, uncoordinated, and disconnected from the digital transformation strategy.
- Digital and data skills that fall under IT specialists but should be skills every employee learns.
- Outdated skills development and recruitment processes.
- A reactive and risk-averse work environment, which should instead be dynamic and innovative to attract the best talent.
- An employee experience that does not provide fulfilling, rewarding jobs or that doesn't create a sense of purpose.

The Chief Digital Officer Solution

Within the government, most leaders don't come from a digital or technology background. And really, there's no reason why they should have intimate knowledge of how to digitally transform an organisation, let alone have the bandwidth to drive those programmes. Instead, the DG or CEO often recruits someone specifically for digital leadership roles, such as a Chief Digital Officer (CDO).

CDOs have achieved a great deal in the government transformation space. Their appointment alone, at a senior level, was a statement that something different was happening, and they have successfully brought in new ways of working, and challenged the status quo, particularly in relation to IT. As digital transformation has become acknowledged as the primary strategic priority for many organisations more 'Ds' have since been added onto the job title. As they took over from IT, which had traditionally been led by a CIO, we saw the evolution of the CDIO. This then became CDDIO as the word data was added in.

Bringing together all facets of an organisation that deal with service design, software engineering, technology and data has merit. Although it should be noted that no one can be an absolute expert across all those domains, so the quality of the team below the CDDIO is critical.

However, even the best CDDIO cannot change HR policies. They can't rework budgeting and financial processes. They can't change the working arrangements of staff, or directly influence the board if they are not

on it. They can't change the communication and working style of executive directors. They can't refresh the job evaluation scheme and pay grading. They can't change the governance cadence of the organisation. In short, outside of building online refreshed government to citizen services, there's a lot they can't do. At least not on their own. This may be a reason why they seem to move from department to department roughly every 18 months. There is a certain amount you can change but without executive level intervention, the CDO runs out of road.

What Does Leadership Failure in Digital Transformation Look like?

As with the digital skills gap the consequences of weak digital leadership can feel somewhat abstract. It's therefore useful to describe a specific example of how it can occur in the day to day delivery of business.

A central government agency set out an ambitious digital vision outlining how it would rebuild all its data and archive assets to make them accessible online and add data and search features.

However, this agency historically had huge difficulty with the recruitment process. After internal processes, union consultation, security checks and the interview process, it took this organisation three to six months to hire even a standard employee. They had never employed software engineers, product managers or modern business analysts before. Their location was an issue when attracting talent, as were pay bands.

Their new strategy described how it would establish in-house, multidisciplinary digital delivery teams working to an agile methodology to deliver the new services, in line with published milestones and associated dates.

Small, multidisciplinary agile teams work to and track their velocity. If a team of seven is down by three software engineers for eight months through churn and slow recruitment, their velocity will plummet. If management insists on observing the same timelines then some or all of the following will happen:

- Quality will be cut to maintain velocity, causing UX issues and possible security risks.
- The team will burn out, especially the engineers. They may leave, worsening the problem.
- The product will not go into production.
- The organisation will have to spend large sums of money on external suppliers to deliver the product and quality may still be cut due to delays.

This example is real, and all the above happened. This was despite the CEO and Board being shown, in quantitative terms, that this was happening. The CEO was asked directly "have you ever intervened with HR to try and expedite the hiring process?" The answer was a resounding "no".

This very practical abdication of leadership responsibility for enabling digital change is literally the reason why digital transformation has not achieved more across government.

This is just one way that poor leadership undermines digital success - it occurs in many others each day in the hundreds of decisions and acts taken by leaders, as well as in their failure to take action. The best digital specialist hired from the private sector cannot overcome that. Bureaucracy, speed of governance, politics and legacy processes within the public sector prevent transformation programmes from achieving widespread momentum.

Many digital transformation projects fail because the executive leadership team behaves as if they have nothing to do with them, beyond signing off a strategy and recruiting a digital leader. Public sector leaders publicly talk of transformation, but, beyond the DDaT team, the culture often remains the same: hierarchical, top down, sclerotic.

When fundamental change is required, this is a failure of leadership.

Implications for Defence and Data Transformation

As referenced elsewhere in this paper, transforming to become a data-centric organisation is likely to be harder than digital transformation. Digital transformation, as it is currently perceived in government, can take place to the side of an organisation without entirely unsettling the established ways of working of the wider workforce. But to achieve a return on investment with data the entire workforce has to be involved. They must learn new skills and absorb some level of practical change to how they work.

Additionally, the stakes for Defence in the UK are higher. Some other countries' defence sectors are ahead of the UK in their experience and use of data and related emerging technology. These countries are not necessarily friendly states. This puts considerable urgency on Defence's ability to become data-centric, as it potentially carries a level of existential consequence. This threat level has been absent from most generic digital transformation initiatives undertaken in government.

Delivering the UK Digital Defence Strategy will therefore require a herculean leadership effort, a hunger to learn and preparedness to question orthodoxy.

Key Takeaways

Becoming a data-centric organisation means building a data culture. The culture - which can only be built and scaled from the top - must value the creativity and artisanship of great software and data engineering, encourage a product mindset, and emphasise user centricity. The leadership team must be empowered with a strong understanding of data business models, a rigorous grasp of the associated technology, and their own respective roles in enabling such an environment.

This requires active leadership, role modelling, communication and investment in line with the following principles:

- Ideally a third of the top leadership teams across the defence family of agencies should be deep software and data experts.
- The main board should have two directors with software and data science experience.
- Measurement of software progress against the data programme should be monitored at board level.
- Engage with HR from the start to understand talent needs and identify those constraints that can be changed and those that can't. A realistic talent plan needs to be developed in partnership with the People Director.
- Senior management must be educated, but this means getting past basic training and visits to start ups. Training must be sufficiently robust and focus on their role in enabling defence to succeed with data.
- Consider inviting software and data leaders in industry to join the board and offer senior defence personnel the opportunity to gain experience in those companies.
- Experimentation is useful for learning, but leaders must determine and signal that they plan to scale. It's easy to get stuck in dashboarding, visualisation and the descriptive layer of analytics.

A Final Thought on Leadership

If you're the CEO of a government agency, your job is to unblock the path of the experts you bring in to deliver your strategy, as much as is practically possible. This is particularly relevant for Defence, where true data-based reform will be even harder than digital transformation. If data experts arrive from industry and then sink in bureaucracy, red tape, and legacy working practices, it's likely they'll leave within a year or two and leadership will be back at square one – having lost precious time.

Section 5: The Digital Culture War

"When it comes to digital transformation, we've transformed the important but simple. And left entirely untransformed, the difficult and the strategic."

Tom Goodwin

As we've already explored in this paper, GDS was created in 2011 to address the very serious challenges inherent in public sector technology delivery at the time. In a pre-GDS world, government-procured services through long term contracts spanning multiple years, focused on technology choices instead of the outcomes they wanted to see, and realised projects through inflexible waterfall delivery methods that could not respond to changing needs and priorities.

With the advent of GDS came a brave new world of user-centrism, where the requirement to consider user needs became the dominant focus in the creation of services, where projects were delivered via agile methods that enabled them to change focus as needed, and where effective feedback loops supported the continuous improvement of products and services. Add to this the responsive centralised spend controls and the G Cloud procurement framework, the state of government digital and technology provision began to look much more positive.

As the saying goes, 'that was then and this is now'. Over a decade later, and GDS style delivery practices have barely evolved even in spite of huge technological and societal change. A strict adherence to these principles is often observed in government, to the extent that the method can become more important than the outcome, in a version of the very approach that GDS was brought in to mitigate.

This does not set the stage well for data, and for the successful exploitation of data that modern public sector organisations need.

From a distance, it might appear that data is merely a subset of the kind of digital transformation we have widely seen across government services in recent years. But whilst there may be some overlap, data is both culturally and technologically different to digital. In order to 'do' data successfully, organisations must consider domain needs and not just user needs, which in a public sector context necessarily means considering policy, strategy and culture more widely and more comprehensively than is common in government digital transformation.

As anyone who has ever undergone any kind of change management process knows, culture is often the most nebulous and difficult thing to get right. In the 10+ years since the advent of GDS, many of those involved in government transformation would argue that there is a strong culture of digital in the public sector - and perhaps particularly so in central government. They are rightly proud of what they have achieved, and the

improvements to service design and delivery that citizens enjoy as a consequence. However, this digital culture, and these newly designed services, for the most part exist in isolated pockets of government such as DDaT teams, who are responsible for building standalone, transactional solutions that enable citizens to complete discrete tasks. However digital these teams and these services may be, they are not the same as the true and fundamental digital transformation of an organisation, or the public sector as a whole. In other words, there are parts of government that are digital, there are parts that very much are not, and there is not much interplay between them.

Data simply does not play according to these rules. In order to reap the benefits of data, an entire organisation needs to be involved and invested in it, as part of a true data culture that considers people, processes, technology, systems, and governance at all levels, in all operations, and at all stages of work. Organisations need to create a highly compelling picture of why data is everyone's job, why it matters to everyone, and why everyone needs to be involved with it on a level footing.

If we paint this picture, we see that the kind of transformation needed for an organisation to become data driven brings everyone in the organisation - including previously siloed digital teams - together around a mutual shared goal. This is consuming, processing or managing data in some way for the benefit of the organisation.

- **Product teams** (designers, researchers, software engineers) - use data to inform, build or improve their products and services.
- **Data engineers** - ingest, transform and aggregate data so it's ready for use in the organisation.
- **Data scientists** - model, develop hypotheses and interpret data to serve up to others in the form of business intelligence.
- **Everyone else in the organisation** - uses data to make better business decisions.

This demonstrates why data is truly transformational, as it touches all areas of an organisation and requires everyone to adapt to a new culture and ways of doing things. It also demonstrates why data is hard, why it's expensive to get right, and why so many organisations are so far away from where they need to be in both their thinking and practices around data.

On a positive note, thinking about data in this way allows us to appreciate the very real and very exciting opportunities that await for organisations that are willing to take on the challenge. As time passes, this will become less and less of a choice, and those that don't will fall behind at an ever increasing pace.

Conclusion

The ambitious transformation strategies published by the MoD position data as core to its operational future. As the strategies note, it is through the considered exploitation of data that the MoD will become more efficient, and more effective at countering evolving security threats. This is also the only way for the MoD to embrace technologies such as AI, which is critical to the UK's ability to secure and defend itself in a world where other actors are moving quickly in this space.

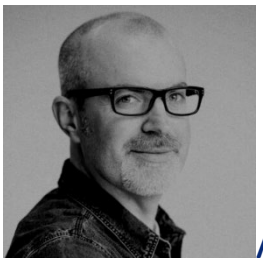
The release of these strategies is a welcome first step in acknowledging the challenge in hand, however they are meaningless without practical action.

By examining the state of digital transformation within the defence sector we can see that it lags behind the rest of the public sector in terms of progress. Defence has largely been insulated from the technological and cultural changes made across government since the creation of GDS over a decade ago, which have helped teams to deliver improved products and services that better meet the needs of their users.

This being said, it has been possible for digital teams in government to successfully take on this work without the need for the broader, more fundamental transformation of public sector institutions – the likes of which is now necessary for the exploitation of AI and data science. So, even though the wider public sector has delivered digital transformation programmes, confronting challenges across procurement, technology choices, digital skills, leadership and culture, the playing field for defence is perhaps more level than it would initially seem.

Defence therefore not only has an opportunity to learn from the lessons of its public sector peers, the details of which we have explored in this report, but also to lead the way with a bold new approach.

By turning the principles of its strategies into a reality through the right partnerships, technology, skills, culture and - most importantly, leadership - the MoD can become truly data driven and set the standard for the rest of government to follow. The opportunity is there: the challenge now is to make it happen.



About the Author

James Herbert, CEO Pivotl

James is an entrepreneur specialising in starting and scaling modern software and technology services businesses.

In 2017 James co-founded The Panoply, which listed on the London Stock Exchange in 2018. Now over 600 people strong, The Panoply delivers Design, Software, Cloud and Data services to global clients across multiple sectors including media, government, energy, financial services and logistics.

Prior to his entrepreneurial career James played a leading role in many of the most significant data and technology initiatives in the UK government. He worked in the Cabinet Office team that designed the G Cloud procurement framework, co-wrote the world's first national Government Cloud Strategy and developed the data model underpinning the NCA.

For more information, please contact: info@ddrc.uk

www.DDRC.UK

DDRC
DEFENCE DATA RESEARCH CENTRE