National Audit Office

REPORT

The Digital Strategy for Defence: A review of early implementation

Ministry of Defence

SESSION 2022-23
19 OCTOBER 2022
HC 797

Key facts

£4.4bn

estimated spend on digital in 2021-22 by the Ministry of Defence (the Department)

£11.7bn

how much Defence Digital estimated in 2019 it will spend updating or replacing legacy technology over the following decade

£2bn

total cash-releasing efficiencies Defence Digital intends to find for the Department by 2032-33

£1.7 billion	the estimated amount of the Department's £4.4 billion 2021-22 digital spend that is outside the direct control of the chief information officer
200,000	users in the Department and the Armed Forces
66%	percentage of Top-Level Budgets' 2022-23 digital alignment tasks which are on track for completion or face only minor issues
55 to 2 minutes	the change in call waiting time for the IT service desk between October 2021 and May 2022
78%	the proportion of significant project delivery milestones Defence Digital completed successfully in 2021-22
151	people with high-priority technical skills that Defence Digital is currently aiming to recruit

Summary

1 The nature of modern warfare is changing, with access to and exploitation of information becoming vital to securing military advantage. The government's Integrated Review placed greater priority on identifying and deploying new technologies faster than potential adversaries to enable operations across all arenas of warfare and collaborate better with partners. Cyberspace is itself also becoming an increasingly important arena of warfare, with external threats increasing and constantly evolving as access to offensive cyber capabilities becomes easier.

2 The Ministry of Defence's (the Department's) assessment is that it needs to keep pace with adversaries in adapting to this shifting technology landscape, but that it is not set up to implement digital technology at speed and scale. Like many government departments, its digital estate contains many aged ('legacy') systems, with resulting operational and cyber security vulnerabilities.[1] The Department holds vast amounts of data, but those data are not easily accessible across its different component bodies. It also has gaps in critical skills and its organisational processes are not always suited to best delivering digital technology.

3 To address these challenges, the Department has developed the Digital Strategy for Defence (the strategy), which describes how it intends to transform its use of technology and data. The Department aims to achieve three strategic outcomes by 2025, which are:

- a digital 'backbone' – this is how the Department describes the technology, people, and organisational processes that will allow it to share data seamlessly and securely with decision-makers across all the military and civilian domains.
- a digital 'foundry' – a software and data analytics development centre. This will use the capability and access to data provided by the 'backbone' to rapidly develop digital solutions in response to emerging needs; and
- an empowered digital function – a skilled and agile community of digital specialists who will help deliver digital transformation and closer integration across Defence.

4 The Department hopes that, collectively, these will help realise its vision for 2030 of allowing users across all Armed Forces and Defence organisations to access and use the data they need without barriers, and better support more joined-up decision-making.

1 Legacy refers to systems and applications that have been operationally embedded within a business function but have been overtaken by newer technologies or no longer meet changed business needs.

5 The Department's chief information officer (CIO) leads Defence Digital, an organisation within Strategic Command. The CIO sits on the Department's Executive Committee and reports jointly to the commander of Strategic Command and the second permanent secretary, who holds senior accountability for digital across Defence. The CIO and Defence Digital lead the digital function, which ensures that digital activity is coordinated across the Department and its Top-Level Budget (TLB) organisations. The CIO and Defence Digital are responsible for leading the implementation of the strategy, with support from TLBs, through a portfolio of organisational change and technology upgrades.

Our report

6 Our report examines whether the Department is on track to achieve value for money in its implementation of its digital strategy. To do this, we would expect the Department to:

- have put in place an appropriate strategy, considering its strategic context and existing digital estate, drawing on good practice;
- have made initial progress implementing the strategy in line with a delivery plan, which allows it to measure and coordinate progress; and
- be working to address the biggest barriers to success and know how it will prioritise its resources and people.

7 Our report is in three parts:

- Part One looks at the Department's strategic context, digital estate and the Digital Strategy for Defence.
- Part Two examines the Department's progress with implementing the strategy.
- Part Three considers key challenges to the Department's implementation of the strategy.

Scope of our work

8 Our report focuses on the May 2021 *Digital Strategy for Defence* and the Department's implementation of it. We, therefore, considered performance information between its publication and our cut-off point for reporting of 30 June 2022 (except where otherwise stated). We have not performed a detailed review of the Department's performance on previous digital strategies or programmes, except to the extent it continues to deliver them as part of the current strategy.

9 Our scope includes the whole Department because, although Defence Digital is responsible for leading implementation, the strategy is intended for all of Defence. We do not draw a distinction in our scope between core IT infrastructure and deployed military technologies, as modern warfare requires the seamless movement of data and applications between these spaces. The Department's ambition is to create the infrastructure and organisational capability to do this.

Key findings

The Digital Strategy for Defence

10 Implementation of the strategy will help the Department to operate more effectively in an era of disruptive technology and evolving security threats. The government and Department have set out in several strategy and policy documents that the nature of warfare is changing. In response, the Department aims to join up military operations across land, air, sea, space and cyber and work closely with the rest of government, academia, industry and international partners. The Department has recognised that data are fundamental to achieving this integration and that it needs to transform its digital capabilities to be secure and easy to use so that it can share information seamlessly and make decisions based on data (paragraphs 1.2 to 1.4 and Figure 1).

11 The Department's assessment is that to keep pace with the increasing capabilities of adversaries requires a fundamental reset of its digital capability. The Department's diagnosis is that its data are hard to access and share, it has gaps in critical skills, its core technology needs updating and its organisational processes are out of date. This is consistent with our wider work on the reasons government finds digital change challenging. The Department has a large legacy IT estate and upgrading to modern replacements is complex. Defence Digital estimated in 2019 that it would spend £11.7 billion over a decade updating or replacing systems, although this figure does not encompass all of the Department's legacy estate (paragraphs 1.5 to 1.7 and Figure 2).

12 The nature of the Department's business adds additional challenges to implementation of the strategy. The Department works across three security classifications (Official, Secret and Above Secret), which sometimes requires it to develop separate systems for each. The Department uses its technology in hostile environments with limited connectivity, such as at sea. This adds to the challenge of modernising and integrating technology. Adversaries also may be actively looking to degrade its digital and military capabilities. The Department shares data with international partners and must be able to work with their technical solutions and security policies (paragraphs 1.8 and 1.9).

13 The Department's digital strategy is consistent with good practice. The strategy states the Department will focus on technology, people, processes and cyber security so that it can securely and seamlessly share and exploit data. Importantly, the strategy recognises that data are a strategic asset and that people and processes are as vital as technology to successful digital change. Both wider government and the Department have been slow to implement digital strategies previously. However, there is strong support for the current strategy from the most senior leaders of the Department (paragraphs 1.10 to 1.14 and Figure 3).

Progress implementing the Digital Strategy for Defence

14 The Department does not have a complete plan to implement the strategy or a clear way of measuring whether its implementation of the strategy is on track. Although the Department has individual plans supporting each of the individual workstreams and programmes, it has not brought these together to provide a complete picture of progress across the strategy. In our work on implementing digital change across government, we have stressed the need for an overall plan for how an organisation can transform itself that clearly sets out the associated ambition and risk. Such a plan would also allow the Department to prioritise its activity effectively when delivery challenges emerge (paragraphs 2.2 to 2.4).

15 The Department has substantially improved the governance of its digital function, which has begun to align Defence organisations to common digital standards and approaches. To create the coherence of digital activity needed to realise the strategy, the Department has developed common approaches and standards for aspects such as data, technology architecture and cyber security. For example, a new Chief Data Office has developed a Data Strategy and rules for formatting and managing data to make them more accessible and usable across Defence. The Department has also established governance to oversee the adoption of these standards across its business, which for 2021-22 it assessed as working effectively with only minor weaknesses. However, the changes required to comply with these standards are substantial, and currently at an early stage. For example, the Department has not yet fully mapped its legacy estate, and not all technology teams have adopted the new standards. Defence Digital sets TLBs annual tasks to improve digital coherence across the Department. For 2022-23, TLBs reported at the end of June that they are on track, or face only minor issues, with completing 66% of them. However, they face moderate issues with, or are at risk of not completing, 29% of them (paragraphs 2.5 to 2.11 and Figures 4 and 5).

16 The Department has improved its core IT services and has plans to improve services further. In 2015, the Department assessed that its users' experience was unacceptable: its operating system was out of date; users had limited storage and collaboration tools; and its devices largely did not allow mobile working. As a result, the Department amended its core IT service contract to progressively roll out upgrades, such as an improved core IT system (MODNet), new software and mobile devices. While the Department judges that its core IT is now fit for purpose, it concluded that the contract was too large, insufficiently transparent to understand user experience, and lacking in levers to improve services further. It is now breaking the contract up and procuring its constituent services separately, which it will integrate itself. The new user service desk introduced in October 2021 supports this effort, by gathering information to spot common problems and address them faster. Following the introduction of the new service desk there was a fall in service performance, but it has recently begun to show improvement in service call waiting times and incident resolution times (paragraphs 2.12 to 2.14).

17 Defence Digital's historically poor reputation for project and programme delivery has been a barrier to integrating digital activity across Defence. Defence Digital has a portfolio of more than 90 digital projects and programmes, including larger and more complex major programmes, many of which it needs to replace fragmented legacy systems and older software with newer capabilities. Defence Digital's project delivery has suffered from a lack of skilled and experienced personnel, immature project controls, and a culture focused on the approvals process rather than outcomes. TLB CIOs told us that this undermined trust in Defence Digital's delivery of the strategy and incentivised them to maintain or produce their own separate capabilities for certain requirements, rather than rely on shared ones delivered by the Department (paragraphs 2.15 and 2.16, and Figure 6).

18 Defence Digital has recognised the weaknesses in its project and programme delivery and is taking action to begin improving them. Defence Digital is resetting its project delivery organisation with improvements including better management information and reporting. The effects are not yet clear in its performance, which the COVID-19 pandemic has also affected. In 2019-20, Defence Digital completed 76% of its most important project delivery milestones, but this fell to 57% in 2020-21 before recovering to 78% in 2021-22, with the Department aiming to increase this to 90%. As of June 2022, two-thirds of projects across its total portfolio reported delivery confidence ratings of green or amber-green, a level it has broadly maintained since the end of 2020-21. The delivery of its major programmes has remained challenging; the Infrastructure and Projects Authority (IPA) publicly rated five programmes for 2021-22, of which three programmes were rated amber, and two red.[2] Defence Digital has further plans to improve delivery, including through additional technical training for its delivery staff (paragraphs 2.17 to 2.19 and Figure 6).

2 The IPA produces an annual report that assesses the likelihood of government major programmes achieving their aims and objectives on time and on budget. A 'red' rating means successful delivery appears unachievable; 'amber' that successful delivery appears feasible but that significant issues exist requiring management attention; and 'green' that successful delivery appears highly likely with no outstanding issues that appear to threaten delivery. Across its portfolio of programmes, Defence Digital internally uses a similar rating system that adds amber-green and amber-red as two further possible ratings.

Strategic challenges

19 To make the strategy affordable Defence Digital increased its efficiency targets and reviewed its costs, which it found to be lower than it originally forecast. The Department had not fully funded the strategy when it published it in May 2021. There was a short-term funding gap for digital transformation of £248 million and an additional £260 million needed for the Digital Foundry. During 2021-22 Defence Digital and Strategic Command worked together to identify funding for the strategy and address wider financial pressures on Strategic Command. Defence Digital considers the strategy affordable following the Department's annual budget cycle in March 2022, which prioritised allocating funding to the Digital Foundry. As part of the annual budget cycle Defence Digital found funding for the following few years by reviewing and refining cost forecasts which decreased by £190 million; increasing efficiency targets by £160 million; capitalising £110 million of resource expenditure; and stopping £60 million of lower-priority work. The Department is likely to continue to experience funding challenges for digital transformation: it may need to fund new capabilities; it may underperform against efficiency targets; and it may experience future cost increases (paragraphs 3.2 to 3.4, 3.9 and 3.10).

20 Defence Digital is on track to exceed its efficiency targets for this Spending Review period and aims to identify up to £790 million more by 2032-33. Defence Digital has formal targets for £1,370 million of cash-releasing efficiencies by 2032-33 but has ambitions to go beyond this and make £2 billion. In June 2022 Defence Digital forecast making £1,215 million of cash-releasing efficiencies between 2023-24 and 2032-33. In the first two years it expects to overachieve against the formal target. However, over the 10-year period it still needs to find £160 million to meet its formal target and £790 million to match its full ambition, and is continuing to work on doing so. It plans for efficiencies to come from workforce transformation, supplier management, automation and data centre rationalisation. Defence Digital's performance in increasing efficiency will affect the funding available for the Department to invest in its priorities, including the strategy, and to address future financial pressures (paragraphs 3.5 to 3.10 and Figure 7).

21 The Department does not have enough people with the right digital skills, which is affecting delivery of the strategy. There is a digital skills shortage across UK industry and the public sector, and the Department finds it hard to recruit and retain talent. This is because the Department cannot match private sector pay, and not all TLBs have the authority from the Department to apply pay uplifts for digital specialists, which is creating internal competition. Technologists see the Department as bureaucratic and the hiring process, including getting security clearance, takes too long. The Department also finds it increasingly difficult to recruit digital specialists to work in Defence Digital's main location in Corsham – it intends to make working flexibly the default to help with this issue. The shortfall of technical skills is affecting the delivery of both individual programmes and the strategy as a whole (paragraphs 3.11 to 3.15 and Figure 8).

22 Defence Digital is trying several initiatives to fix its skills gaps, but its progress has not been fast enough to match the problem and a different approach is required. Our wider work across government suggests that, based on its current plans, the Department will find it difficult to make progress on this issue at the pace it wants. Defence Digital's 'Digital Skills for Defence' programme aims to enhance digital skills across the Department for its digital professionals, leaders and the remaining workforce. Defence Digital is tackling its own workforce challenge by recruiting for technical skills, investing in training, removing legacy roles and reducing the contractor workforce. This activity has taken it longer than anticipated, due to the complexity of developing a workforce plan, and it has begun implementing key elements while it finalises this plan. By June 2022, it had hired 42 of the 151 people with critical skills that it wanted and was in the process of bringing in 39 more. Defence Digital has 3,090 workers, of whom 570 are contractors (18%). It intends to reduce workforce costs further, through organisational restructuring and by reducing the cost of contractors. Defence Digital has started extending its approach to TLBs, who are largely on track to align with it, but still face their own issues acquiring skilled people (paragraphs 3.15 to 3.19).

23 The Department's CIO and Defence Digital are accountable for leading the implementation of the strategy, but they do not have all the organisational levers needed to do so. The CIO is accountable for the whole Department's use of technology and data but only has direct control of £2.7 billion of Defence's estimated £4.4 billion digital spend. There are business changes needed to realise the strategy, which the wider Department will need to deliver. For example, the Department's lengthy approvals and acquisition processes do not suit the more iterative approach favoured in technological change. The Department's senior leadership has recognised that trying to influence the wider Department through the digital function is not enough. The Department is now addressing this as part of its agenda to exploit digital for wider Defence objectives (paragraphs 3.20 to 3.23).

Conclusion on value for money

24 The nature of modern conflict is rapidly digitising, affecting the Department's business and how the Armed Forces operate in the battlefield. The Department has put in place a digital strategy to respond to this challenge, which is consistent with good practice, has provided clear direction across the Department and has support from the most senior Defence officials. The Department has made good progress with bringing together and aligning digital practitioners across Defence. However, its performance in delivering major digital technology programmes needs to improve and is a risk to achieving this alignment.

25 The Department does not have a complete picture of its progress against the strategy and so cannot readily demonstrate whether it is on track to deliver it or not. To meet the needs of the modern battlefield, and enhance its business efficiency, the Department must transform a large and complex organisation with an extensive legacy estate, using scarce specialist skills. Given the scale of the challenge and the persistent barriers to change, achieving the strategy's objectives by 2025 is ambitious. As future delivery challenges emerge, it will be important for the Department to prioritise its funding and specialist skills to where it needs them most urgently. The Department will be able to do this more effectively if it can articulate better how it will achieve the strategy's vision in practice and how it will measure success along the way, not least in supporting its wider departmental objectives. This will allow it to achieve greater value for money with its £4.4 billion of annual digital expenditure.

Recommendations

26 Our recommendation aims to support the Department as it attempts to implement the strategy by its target date of 2025. We recommend the Department should immediately create a clear delivery plan for the digital strategy which:

- integrates the strategy with wider efforts to transform the department, deliver efficiencies and exploit technology;
- identifies and prioritises all the activities needed to achieve its strategic outcomes;
- identifies what people, skills and funding it will need to deliver these;
- develops a set of leading indicators to show the prospects for future progress; and
- sets out and agrees a consistent set of performance information for use across the digital function and the wider Department.