Strategic Defence Review 2024
Call for submissions - techUK response

1. About techUK & Summary of Submission

1.1 techUK is the trade association which brings together people, companies, and organisations to realise the positive outcomes of what digital technology can achieve. We create a network for innovation and collaboration across business, Government, and stakeholders to provide a better future for people, society, the economy, and the planet. techUK represents over one-thousand-member companies working across the UK technology sector.

1.2 techUK welcomes the opportunity to provide written evidence to the 2024 Strategic Defence Review (SDR). Our submission is based on inputs received from techUK's member companies with interests in Defence and Security matters, ranging from multinational technology companies, prime manufacturers, consultancies, and SMEs, addressing those SDR propositions to which our members are qualified to provide insight and positive contribution.

3. SDR Proposition 3

3.1 Information is critical to all the MOD's military capabilities and the efficiency of its corporate services. However, Defence acquisition over the past decade has remained platform centric, with digital elements often regarded as an afterthought rather than a fundamental. This platform centric approach has meant that the MOD has not prioritised investment in battlefield management systems, communications software, and other digital technologies, all of which are fundamental to success in conflict. techUK believes the MOD must shift from a platform centric to a data centric approach when prioritising future capabilities. Getting this right will be a force multiplier, helping maintain the UK's competitive advantage.

3.2 An information-first policy should also focus MOD investment on addressing cyber security threats and resilience vulnerabilities. Several techUK members shared specific examples of where networking architecture is not securely designed, meaning for instance virtual private networks (VPNs) and encryption cannot be used to secure systems currently in operation (such as UAVs).

3.3 The UK must also decide what capabilities it wishes to regard as sovereign, building and operating alone, and which it does through coalitions such as AUKUS, 5 Eyes and NATO. Critical determining factors must be capacity and affordability, not unrealistic aspirations to do everything.

4. SDR Proposition 4

4.1 The MOD must urgently invest in digital capabilities to address its growing obsolescence and technical debt issues. It faces a burgeoning problem of late running programmes and must address where obsolete and legacy IT programmes remain in operation. This must include a systematic review of the systems MOD operates, including life expectancy and contract terms.

4.2 As an example, a techUK member cited the MOD's continued use of Skype for Business, a system that falls short of current requirements for secure communication and does not offer flexibility or integration with advanced policy controls.

4.3 On the MOD's Secure by Design policy, techUK members expressed frustration that there is not enough knowledge within the department to have intelligent customer conversations, and that it is not clear that MOD knows what it wants. Members noted there is no transparency or consistency on tolerance of risk around obsolescence (with an impact on security – e.g. inability to patch software) and the reasoning behind decisions is not clearly communicated. Companies supplying the MOD are being asked to shoulder risk without clarity on both tolerance of risks and ownership of them.

4.4 When identifying and addressing urgent cyber security and resilience risks the MOD must consider the entire Defence enterprise, including the Department's whole supply chain. Not doing so risks allowing vulnerabilities within the enterprise, inevitable primary targets for potential adversaries. In addition, with growing demand across HMG for more At Secret and Above Secret infrastructure, this widens the vulnerability for Government in being able to rapidly secure the necessary technical equipment and resources when required.

4.5 The MOD as a 'second mover', should take advantage of where others are already leading. Zero Trust is a good example where huge investments have been made by the US DoD and a consensus is emerging around what the most successful architectures look like.

7. SDR Proposition 7

7.1 There are considerable opportunities for integration and shared capability across secure government; yet despite similar requirements, there is too much duplication of work (or 'wheel re-inventing' as one techUK member described it). The MOD should lead on creating a joint, single list of definitions for technical and acquisition terms used across the secure government space, making it easier for itself and industry to operate as one. It must then look to develop common tools including a single Collaborative Working Environment and secure cloud environment(s) to operate across the Defence and National Security space, with common or joint procurement processes to simplify and ease acquisition.

7.2 Further barriers to information sharing include Identity and Access Management (IdAM) and problems around mutual recognition of security clearances. techUK members have suggested that data-centric access controls rather than an infrastructure-led approach to systems design (zero trust) would significantly smooth this process, utilising digital identities and role-based data access controls. Such an approach could save significant amounts of funding duplicating elements of the technology stack at different classifications.

7.3 Finally, techUK members have noted that the classification (or overclassification) of data is a barrier to collaboration and information sharing. One member raised satellite imagery as an example of where security classification prevents broader sharing across the Defence and National Security estate.

8. SDR Proposition 8

8.1 techUK sees a Multi-Domain Force as an evolution of the prior concept of Campaign Componency: operating domains each with a strategic proponent, capability sponsor, operational commander, and each effectively siloed. Advancing to an Integrated Force needs lateral integration across domains at all levels of command and control (C2), with operational activities exercised by humans and machines at the time and place required (including “at the edge”).

8.2 Integrated Force capabilities must be designed with an information architecture as a prerequisite, to plan the delivery of any effects, kinetic or otherwise. Technologies, sensors, systems, and platforms are designed around the data required to deliver an effect. A standardised information environment onto which these integrate allows rapid technology insertion and innovation.

8.3 techUK argues that this all requires coherence of capability sponsorship, with an authoritative operating model throughout the capability lifecycle that designs and enforces (or otherwise) the appropriate integration. It needs an architecturally led acquisition model driving investment priorities and performance management of delivery across all domains.

9. SDR Proposition 9

9.1 The MOD must first define what is meant by Defence homebase in this context. It is widely accepted that in any conflict, adversaries will first target Critical National Infrastructure (CNI), not just Defence, but there is no coherent strategy within HMG to defend against this type of attack. Whilst there are no doubt physical threats to national Defence infrastructure and capabilities, early attacks will be cyber-based and therefore more effort should go into bolstering of the cyber resilience of CNI, which includes the MOD and its assets.

9.2 techUK members believe that operating separate environments for operational cyber capabilities and threat response duplicates effort and risks creating gaps through which threats can penetrate. Therefore, techUK would like to see the MOD merge further the Network Operations Centre (NOC) and Security Operations Centre (SOC) duties, allowing service-affecting issues to be viewed through a cyber lens and vice versa.

9.3 Industry partners can do more to replace scarce Government skills, including with AI-driven automation already on the market to help optimise this challenge. The MOD should also look at the creation of specialist Digital skills reservist posts for deployment in times of crisis.

10. SDR Proposition 10

10.1 techUK members have noted that the MOD’s enterprise architecture lacks coherence and that the department is not fully aware of what systems it operates. techUK would recommend the MOD conduct a comprehensive review of its architecture and CMDB to enable a better understanding of where it stands with legacy systems, interfaces and to help identify where shadow IT is being used.

10.2 techUK members also cited a lack of proper network integration continues to prevent distinct parts of the MOD (DE&S, Dstl, Main Building, etc.) and suppliers from communicating with each other securely. One member expressed frustration at their continued reliance on Defence Courier Services to communicate with the MOD as current systems are not interoperable.

10.3 On the Defence innovation ecosystem, techUK recommends the MOD conducts an immediate and comprehensive review of all innovation units across MOD delivery agencies and Front-Line Commands (FLCs), with the express aim of consolidation. There is wide agreement in industry that there are simply too many, each with their own evaluation and procurement processes, with the funding spread too thinly. Many of these units lack a means to drive technology experimentation into funded programmes of record, with the ‘valley of death’ preventing adoption of emerging technology.

10.4 This complex ecosystem is confusing and risks significant duplication of efforts as innovation units do not communicate with one another effectively. techUK SME members in particular frequently express frustration at the absence of a single innovation ‘front door’ or ‘concierge service’ where companies can present ideas or products, to then be directed to the most appropriate customer(s). To fix this, the MOD requires innovation intelligence across all units to ensure they are not pursuing capabilities that already exist, particularly when those capabilities are based on common technology stacks. Corporate knowledge is not being shared across the Defence enterprise and there are real efficiency savings to be made here if this is implemented.

10.5 To simplify this, techUK members would like to see the MOD appoint a single authority (such as the Integration Design Authority) with the responsibility of overseeing innovation investment, ensuring interoperability and pull-through from one service into others when projects prove successful. AI-based Knowledge Management tooling would also be effective and could easily help save more than it would cost.

10.6 Furthermore, techUK members expressed concern that despite the existence of the Defence AI Centre (DAIC), there is not a single, recognised authority for providing AI assurance across UK Defence. techUK would like to see the whole Defence enterprise recognise the DAIC as having this responsibility, with a clear process for assurance and approval of AI technologies once acquired. In addition, the MOD must not attempt to duplicate work already undertaken elsewhere in HMG, and the process should align with the existing frameworks led by the Responsible Technology Adoption Unit within the Department for Science, Innovation & Technology (DSIT), ensuring compliance with EU AI Act, the US NIST Risk Management Framework and ISO 42001.

10.7 To become a global pacesetter techUK believes that Defence Digital must acknowledge it cannot do everything, and nor should it, and explicitly embrace a Commercial Off-the-Shelf (COTS) based approach as the default. techUK members have suggested that the MOD should not be investing in technologies internally where it does not have either the critical mass or skills and is simply competing with the private sector.

10.8 techUK members believe the MOD needs to learn from how the US Department of Defense pursues commercial arrangements in Intelligence, Surveillance & Reconnaissance (ISR). Members are concerned that the Defence enterprise is not able to access the vast data and imagery available through private sector collection at a fraction of the cost of traditional platforms. The department must continue to invest in these 'non-traditional' collection assets and adapt both its culture and structure to successfully leverage the quantity and quality of data offered.

11. SDR Proposition 11

11.1 techUK members have argued that the MOD should conduct Strategic Supplier Management much more effectively, employing full time, strategic commercial relationship managers as other government departments do. Through constant dialogue, managers would be tasked – and incentivised – to find efficiencies in existing programmes. Members are confident such roles would quickly pay for themselves if implemented.

11.2 To facilitate an enduring relationship with technology providers the MOD needs to maintain a constant dialogue with new and trusted industry partners, sharing challenges so industry can best understand its approach to help us respond in the right way. There are examples of this working well when implemented, such as the adoption of ISO44001.

11.3 techUK members of all sizes also reported a critical lack of parity and experience across both technical, and contracting and administration teams when dealing with complex issues, causing serious delays, and preventing agility from being achieved. Members noted that poor understanding within procurement teams as to what they are buying results in an overemphasis on price and not capability. One member also reported concerns that the Defence Sourcing Portal (DSP) is being circumvented on eligible programmes with contracts going straight to a predetermined supplier.

11.4 The MOD must ensure consistent and regular dialogue with industry but techUK members note that the willingness of technical and commercial teams within Defence Digital to engage is mixed at present. While some teams actively embrace interaction, one member reported reluctance from a specific technical team at the suggestion of engaging externally.

12 SDR Proposition 12

12.1 The UK is home to a DefTech industry with capabilities in data-rich sensor systems (and ready for AI exploitation in defence) including electronic warfare, optical sensing including object recognition, video moving target induction, and Radar. UK industry has considerable expertise in areas such as: delivering advisory services across the whole AI lifecycle; suitably Qualified & Experienced Personnel (SQEP) to deliver supply side AI development projects at scale; integration of new technologies into complex systems; and facilitating the cross pollination of skills from the wider digital technologies sector.

12.2 Despite a plethora of initiatives across the Defence enterprise to improve acquisition and procurement, the view of techUK members is that a fundamental cultural shift in approach is required to achieve meaningful change. Many members expressed frustration at a 'this is the way we've always done it' rather than a positive 'can-do' attitude across the MOD. This is most evident in the calculation of risk, and commercial officers should be better trained to measure this against a list of published criteria.

12.3 techUK would like to see the MOD acknowledge the risk that being an “unattractive client” has on the UK’s sovereign capabilities. SME members expressed frustration at unnecessary and excessive contracting terms and conditions, such as an IT consultancy projects requiring declarations on munitions and asbestos, or where a subcontractor was expected to carry excessive liability insurance.

12.4 techUK SME members noted barriers to business including that security clearances are required to bid for work but cannot be applied for until a contract is in place, and a minimum required turnover set at the value of a potential contract meaning many SME companies are ruled out of MOD contracts and unable to grow in the sector. techUK would like to see MOD commercial officers empowered to know when certain contracting requirements are relevant and when they simply hinder business.

12.5 techUK members argue that the MOD must also be prepared to ‘fail quicker’, citing examples where programmes have continued to receive funding long after the point at which it was clear they were not viable. More regular independent reviews would help address this issue.

12.6 SMEs also raised frustration at the use of frameworks by the MOD. Frameworks place a direct barrier between the MOD and SMEs engaging in necessary dialogue, and each framework operates with different joining processes, and terms and conditions. Limited windows for entry mean newer companies are locked out of the procurement cycle. It is also not clear which framework the department will use when going to market.

12.7 The MOD should consider whether a CAPEX approach to digital capabilities (and related Intellectual Property) remains the most effective way of acquiring services, or whether a supplier-owned and managed approach – ‘as-a-service’ or ‘commercial subscription’ models – would best drive constant innovation and prove most cost efficient. Other government departments take such an approach to IP, allowing contracted companies to grow and expand.

14. <u>SDR Proposition 14</u>

14.1 techUK believes the MOD urgently requires one single authority to oversee architectural coherence, with funding set aside to enable true integration and interoperability across the Defence enterprise. techUK members shared examples of duplicate work such as Collaborative Working Environments and secure cloud infrastructure, which create future integration challenges and cost the MOD significant amounts of money to resolve. Another example raised was the development of the RAF’s Nexus programme by the Rapid Capabilities Office, running separate to the Army’s Zodiac programme under Commercial X.

14.2 techUK would like to see this single authority have responsibility to oversee all innovation units, ensuring that work is not duplicated by separate FLCs, particularly where technologies are built on near-identical stacks. This authority would ensure that successful projects are pulled through into the other TLBs, driving interoperability and improving efficiency.

14.3 This authority would also function as an Inspectorate of IT Standards, with the power to conduct routine and snap inspections of the Defence IT estate, holding to account those using shadow IT and issuing penalties where appropriate. This is standard practice in other industries such as with the Health and Safety Executive.

15. SDR Proposition 15

15.1 techUK members of all sizes expressed frustration that commercial teams lack both the technical understanding to have intelligent customer conversations, and the administrative and contractual skills to manage complex contracting problems. This problem is further exacerbated by rapid turnover of staff. One member for instance dealt with three separate commercial officers in a single year.

15.2 techUK believes the MOD should review the training and resources provided to commercial officers to ensure they are suitably equipped to manage the processes they are responsible for. Part of this training review should focus on building substantial partnerships with industry to enable secondments. This would provide industry expertise into the MOD and enable commercial officers to gain an insight as to the actual capabilities of those companies trying to contract with the department.

15.3 techUK members raised examples where delays in contracting have resulted in smaller companies (either directly contracted or in a supply chain) going bankrupt as they wait for the formal processes to be completed. Any education or training review must ensure that MOD commercial officers genuinely understand the impact that this can have on businesses, specifically SMEs.

16. SDR Propositions 16/17/18/19

16.1 techUK believes the Defence enterprise requires clear innovation intelligence authority that understands the needs of each FLC, where it is going to find those technology solutions, is sufficiently empowered to pull through investments into the Centre and into other FLCs. techUK believes the FLCs need to replace their ‘not invented here, not interested’ mindset with an approach that embraces proven technologies, regardless of their source. Members expressed concerns that FLC innovation units work in isolation, risking duplication and wasted investment. Particularly frustrating when those technologies rely on near-identical technology stacks.

21. SDR Proposition 21

21.1 techUK members raised concerns that modern infrastructure including accommodation is not constructed with modern connectivity from the outset. Members cited outdated technologies such as copper cabling still being installed in new properties despite the shift to fibreoptics and wireless in the private sector. This approach simply means that upgrade work will be required sooner, driving up costs.

21.2 techUK believes the MOD should recognise the long-term value in investing in COTS estate management systems to aid intelligence and analytics around estate usage. This will provide a greater understanding of requirements and the pressures that the estate is under, helping advance the sustainability agenda.

21.3 techUK recommends that IoT and OT with data platforms is used to drive efficiency, sustainability and security of the estate.

22. SDR Proposition 22

22.1 techUK believes the MOD at present has no clear understanding of what systems it operates, including the status of those systems' contracts, and where those systems are interlinked. The MOD's priority should be to procure a single COTS, cloud-based centralised Digital Financial Management System to operate across the whole Defence Enterprise. Introducing such a system would allow the MOD to integrate budgeting, accounting, procurement, and reporting functions, providing real-time visibility and control over management information (MI) and financial data.

22.2 With such data to hand, techUK would like to then see Strategic Supplier Managers deploy AI tooling to interrogate existing contracts to examine obligations. Doing so will help identify expensive missing dependencies along with end dates and options and overlaps and increase savings by identifying and removing instances of duplication.

22.3 In addition, techUK believes that the adoption of advanced analytics and AI tools can provide predictive insights into future budgeting, spending patterns, and financial risks. By analysing large datasets, the MOD can make more informed investment decisions, ensuring that resources are allocated efficiently and effectively. This will also enhance transparency and accountability by providing clear, data-backed justifications for expenditure. Automation of routine tasks like invoice processing and expense tracking will also reduce errors and increase efficiency.

22.4 techUK would also like the MOD to provide greater clarity and transparency on procurement and fiscal management initiatives so industry can be part of the solution. There must be analysis undertaken to understand whether the MOD's CAPEX approach makes financial sense given other industries do not operate like this. This should involve the MOD being prepared to look beyond contractor owned and managed, to supplier owned and managed digital capabilities where this could enable greater innovation.

23. SDR Proposition 23

23.1 As part of a constant dialogue with industry, techUK believes the MOD should be prepared to take full advantage of strategic suppliers' presence across allied countries to 'join the dots' with what other nations are investing in, acknowledging that the UK cannot do everything, and must be more proactive in pulling tested capabilities through.

23.2 techUK would like to see NATO learn from the AUKUS experience of bringing together trade bodies and industry through the AUKUS Advanced Capabilities Industry Forum (ACIF) to help build relationships and foster technology collaboration. techUK would like to see the MOD use AUKUS Pillar II as an opportunity to embed interoperable digital technologies into the core of future operating systems.

23.3 techUK would also like to see the MOD continue to address hurdles around mutual recognition of security clearances, work visas, and the ability for companies to share sensitive information across countries. Architectures should include 'open as possible, secure as necessary' cloud-native systems to allow rapid technology and data transfer, and technology insertion.