Written evidence submitted by techUK.

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 1000 member companies working across the UK technology sector.

1.2 techUK welcomes the opportunity to provide written evidence to the committee. We hope that this submission, comprised of input from individual member companies, helps to inform the work of the Sub-Committee on Developing AI Capacity and Expertise in UK Defence.

1.3 The submission is based on inputs received from techUK's member companies, ranging from multinational technology companies, Prime manufacturers, consultancies and SMEs.

2. How clearly has the Ministry of Defence set out its priorities for the kind of AI capacity and expertise it believes the UK defence sector should have, what priorities has it identified, and are these deliverable?

2.1 There is broad consensus among techUK members that MOD (Ministry of Defence) is articulating its priorities in the field of artificial intelligence (AI) and that strategy is well described. The Defence Artificial Intelligence Centre (DAIC) is communicating clearly AI priorities and initiatives. One member questioned the precise role that DAIC is fulfilling when compared to the position outlined within the Defence AI Strategy 2022 with outstanding questions around if DAIC is the focal point for AI research and development (R&D), and if it has the authority to mandate, noting that the Front-Line Commands (FLCs) have established AI Centres or Cells themselves.

2.2 techUK members noted that there remains a disconnect between the MOD's AI strategy and implementation of AI technology in Defence, but agreed that the strategy is driving action and investment in the technology. Members agreed that to expediate AI implementation a clear 'delivery roadmap' covering research and development and procurement is needed. This roadmap should include visible tasking pipelines with robust budgets and dates.

2.3 Several techUK members raised concerns about the MOD's AI ambitions and how these can be realised at the operational level given the lack of common architectural standards, patterns and interfaces across Defence including in the FLCs. Practical details such as a clear understanding of the skills that AI adoption and implementation requires both of industry and within the MOD, how Defence will build and manage data (critical to the operation of AI), and what appropriate controls are in place to ensure technologies are cyber-secure by design, remain to be articulated.

3. **What strengths and expertise does UK industry currently have in the field of Artificial Intelligence with defence applications?**

3.1 techUK members are in agreement that there is a rich ecosystem of AI expertise within the UK which has good connections into the Defence supply chain, sharing an appetite for solving Defence problem sets.

3.2 The UK has strong capabilities in data-rich sensor systems (and ready for AI exploitation in defence) including electronic warfare, machine learning, optical sensing (including object recognition), video moving target induction, Radar, and Sonar.

3.3 In addition to technology, the UK technology industry has considerable expertise in areas such as: the delivery of advisory services across the whole AI lifecycle; suitably Qualified & Experienced Personnel (SQEP) to deliver supply side AI development projects at scale; the integration of new technologies into complex systems; and facilitating the cross pollination of skills from the wider digital technologies sector.

3.4 There is significant technical strength in the UK's small and medium sized enterprise (SME) base, with each SME bringing a unique offering whilst operating at varying levels of maturity. Members also noted that SMEs entering the Defence space do so through different routes: either via Defence and Security Accelerator (DASA) funding or university programmes.

3.5 Members also highlighted the very strong academic-research centres such as the newly established Defence and Security Centre at Oxford Brookes University (DASOBU) that do a good job of drawing together government, academia and the private sector to collaborate on the development of AI technologies.

4. **How can the UK Government best develop capacity and expertise within domestic industry in sectors such as engineering and software to support the development and delivery of Artificial Intelligence applications in defence?**

4.1 Responses to this question from techUK members fall into four broad areas: funding, workforce capacity, data, and standards. On funding, greater incentivisation in the UK Defence sector is essential to achieve the immediate and near-term development of AI applications. This could be through direct funding of technological development, but also through competitions akin to models such as the US Defense Advanced Research Projects Agency (DARPA).

4.2 On funding, techUK members argued that the MOD should focus investment on frontline capabilities with specific Defence applications that are unlikely to be replicated in the private sector (such as Electronic Warfare rather than Natural Language Processing). Members acknowledged that where commercial AI solutions to certain challenges offer better value for the taxpayer they should be adopted in Defence. Examples of this cited by techUK members include AI solutions being developed for the private sector that drive efficiencies in the business operations space.

4.3 On workforce capacity, techUK members stressed that individuals must be engaged in the Defence applications of AI from career-entry through apprenticeships, sponsored university projects and PhDs. To continue professional development and deepen domain understanding, members argued that the MOD should then look at mechanisms to allow individuals to work within the Department through secondments, job-swaps, and being embedding within projects throughout the course of their careers.

4.4 In addition, techUK members agreed that this upskilling must also take place within the MOD so that both sides understand each other better and that AI related capabilities and requirements coalesce faster. AI is a technical subject by necessity, and therefore requirements managers, programme managers and senior responsible owners (SROs) must all have a solid grounding in the technology to drive procurement strategies. Members suggested that to aid this the MOD should also look at its ability to retain talent, including salaries that fall far below industry standards.

4.5 techUK members noted that AI applications must be trained and tested on context-specific datasets, and highlighted the fact that there is huge unrealised potential from focussed collection and brokering of Defence datasets from exercises and operations. techUK members expressed a strong need for access to datasets outside classified environments to stimulate and improve the ability of new companies to enter the Defence sector. Given the levels of military specific context required, unlocking such datasets will allow new AI capabilities to be tailored more effectively to the military domain. This will require a greater risk appetite for sharing real data or investment in generating synthetic data. Members further argued that the MOD should look at building cloud based workspaces on certified platforms to allow collaboration with controlled access to data.

4.6 In addition, several techUK members flagged concerns that each FLC is building its own AI capacity. Not only does this drive divergence and kill economies of scale, but the multitude of Innovation Centres across the FLCs appear to have differing views on IP and ownership around software and AI. Members agreed that a common approach and toolset should be driven centrally by Defence Digital and hosted on MOD Cloud. A UK AI Reference Architecture is necessary to provide a common lexicon and maturity model.

4.7 techUK members also noted that the MOD must ensure the UK's positions on AI remain under constant review within the context of a rapidly evolving technological landscape. Continued close involvement of industry in high level discussions on AI will be important in achieving this.

4.8 On standards, techUK members noted that government (HMG) should also look at standardisation across assurance and technical evaluation processes, including safety and security protocols, ethics framework compliance and simplifying and streamlining processes where possible. Some members suggested that aligning AI standardisation and insisting on this as standard in procurement (as has previously been done to ISO 15288 for systems engineering or ISO 9001 for quality) would be helpful. With reference to intellectual property

(IP), one member raised a concern around DEFCON 703 as disincentivising industry, and in particular SMEs, from doing business in Defence.

5. What can the Government do to help embed UK AI companies in defence supply chains, both domestically and internationally?

5.1 Given the lure of easier and quicker returns on AI investment in the private sector, techUK members expressed the need to see longer term financial commitments to encourage investment from industry in Defence focused solutions. One member raised concerns that their experience of working on AI research and development with Dstl is that projects can 'stop and start on a whim', and are not directly attached to funded programmes of record.

5.2 techUK members strongly agreed that radical transformation of the current procurement model is needed to make the MOD 'AI ready' by 2025. This means that the MOD must recognise frameworks developed for acquiring military hardware are not appropriate routes to market for AI capabilities, especially when the speed at which innovation and technological development of AI is so rapid.

5.3 In addition, techUK members noted that even when rapid testing and innovation is successful, fast deployment of AI capabilities in service does not often follow. Of particular urgency is the need for existing deployed military capabilities to become 'AI-powered' where possible, often at the expense of new programmes that may or may not be delivered on time. There is also a capacity requirement in the internal innovation MOD ecosystem to complete all the necessary tasks around the embedding and integration of new technologies into existing systems. This can be the slowest part of the system, but members argued that a change in the allocation of funds to FLCs to specifically deliver AI enhancements to current operational capabilities would deliver real benefits at pace.

6. How can the UK Government ensure that it champions the UK AI sector in the context of Pillar 2 of the AUKUS Partnership?

6.1 techUK members recognised the generational opportunity AUKUS presents for UK Defence to shape the future of the sector, and if designed properly could present a blueprint for future international Defence collaboration from research through to operational deployment.

6.2 Members suggested that the UK should see AUKUS as an opportunity to lead a unified approach through a common AI Reference Architecture, accreditation process and product/design policy. Members argued that AUKUS standards need to be devised as a priority so that measures are not retrofitted as AI technologies develop, and to ensure that once a new technology is ready to be deployed it is not delayed by the need for further adaptations or procedural bureaucracy.

6.3 At present, techUK members do not feel there is a centre of gravity for AI work within the UK's contribution to the AUKUS partnership, which makes it hard for companies to proactively engage in associated opportunities relating to AI. Some members suggested that responsibility for this should sit with a qualified

centralised body such as the Defence Science and Technology Laboratory (Dstl) or the DAIC. Some members also suggested the MOD should look at creating a framework contract with sub-lots for each Pillar 2 workstream, based on the assumption that each AUKUS partner nation would be running AUKUS related procurements at the national level. This would provide a contractual mechanism for the MOD to engage industry on AUKUS requirements, including in the AI space. It would also allow MOD to present more detailed information on AUKUS goals, targets and deliverables.

6.4 techUK, along with the other main Defence focused trade associations in the UK (ADS Group, MAKE UK and the SMI) is keen to see the MOD supported AUKUS Advanced Capabilities Forum (AIF) play a key role in helping to reduce barriers to cooperation across the AUKUS partner nations, and to provide a conduit for AUKUS opportunities (including in AI) between government and industry.

6.5 techUK members also suggested that the AUKUS partner nations should examine the possibility of running Innovation Challenges for industry, with one member arguing that Electronic Warfare would be a good place to start. Members noted that the first AUKUS AI and autonomy trial held in May 2023 and organised by Dstl should provide a model for future cooperation in AUKUS, as it successfully showcased UK talent and skillsets, and helped position the UK as an innovation and enablement hub.

6.6 However, techUK members agreed that at present there a several fundamental barriers to collaboration in AUKUS. With this in mind techUK members stressed that HMG should look to address hurdles around security clearances, work visas, and the ability to share sensitive information across countries directly with the other AUKUS partner nations. Members agreed that architectures should be ‘as open as possible, and as secure as necessary’, supported by cloud-native systems to allow rapid technology and data transfer, and technology insertion into AUKUS capabilities.

6.7 techUK members acknowledged that work has already been undertaken to reduce the regulatory and legislative barriers between partner countries. However, members stressed that if true technology transfer is to take place across the technology lifecycle, these barriers need to be removed quickly, with a particular focus on the US’s International Traffic in Arms Regulations (ITAR) and the awarding of Open General Export Licences (OGEL).

17th January 2024