Written evidence submitted by BT Business.

BT Group is a European innovation leader and regards AI as a vital future capability to keep ourselves and our customers secure and is committed to the responsible exploitation of the technology. We have been researching AI since the 1980s, and responsibly developing and deploying it since the 1990s. Our responsible AI approach is rooted in our Responsible Tech principles, and built on strong foundations of data governance (cf. BT Responsible AI approach). As a strategic supplier to the MOD, we welcomed the publication of the British Army's approach on AI, and followed closely the development of the Front Line Command Programmes and the Defence AI Centre (DAIC) closely, as well as Government's work around misuse of AI by bad actors and hostile states at the UK AI Safety Summit in November 2023.

The MOD has been challenged to adapt at scale and pace as **adversaries are investing significant resources to utilise new AI capabilities in conflict; including sub-threshold activities and influence operations**.

Unfortunately, **industry investment in AI capability is often not specific to the concerns of Defence**, with private investment being mostly focussed on developing capabilities for corporate or broad commercial benefit, as highlighted in discussions with peer organisations at a recent AUSUK industry event. Besides, hostile attacks against the United Kingdom's public and private institutions have demonstrated that the **general public remain at risk from the fallout of geopolitical events.**

In this context, the Government has rightly refreshed its Integrated Review and we encourage the MOD to broaden its approach on how it **protects the national interest** in the face of adversaries exploiting AI in warfare, with particular focus on enabling capabilities for the MOD within the Critical National Infrastructure (CNI).

The previously published Defence Artificial Intelligence strategy sets a clear approach for developing and exploiting AI skills for UK Defence. The private sector has been investing in AI for decades and competition for skills is fierce. We are pleased to see that the **MOD recognises the role of skills within industry and is looking to further develop its engagement programmes**.

New collaborations through AUKUS, if delivered effectively, could increase the security of the UK and its allies. The provisioning of common platforms for hosting, an accessible compute capability for training AI, secure hosting and networked environments **to facilitate cross country working** should be considered as priorities.

Whilst the MOD may benefit from AI solutions being developed for broader markets, such as logistics, communications and IT, there are more niche applications where it must drive fundamental research. AI development requires investment and dedicated resource to be delivered effectively. Consequently, in order to meet its needs, the MOD should look to work collaboratively with industry to **encourage the development of appropriate technology**. This involves not just investment, but extensive partnerships that share knowledge, data and infrastructure and see fundamental technology developed from concept to product.

BT's internal research shows that the adoption of LLMs has presented malicious actors with a unique opportunity to target society and industry at scale. AI will become not just present in explicit use cases, but **endemic across any IT estate**. Understanding the vulnerabilities and exploitation of AI across the MOD is crucial to being able to satisfy concerns around ethics and risk.

Sovereign AI capabilities will be critical and it is key that the UK works to foster innovation at home. Whilst some funding opportunities for private and academic organisations is available (e.g., Defence and Security Accelerator) we would like to see the MOD increase the collaborative aspect of these engagements and commit to **longer-term bodies of research**. Providing this stability will have the added benefit of encouraging longer term investment by industry. The MOD must remain cognisant of supply chain risks and maintain appropriate standards for vetting for AI development teams (where this is applicable).

The Defence sector suffers from **challenges around suitably qualified and experienced personnel** due to the competitive market and delays in vetting. Investment in longer-term research programmes would give industry greater confidence in engagement with MOD. The MOD could consider creating a specialist unit within the Armed Forces Reserve to bring together AI capability for Defence or further develop existing units, such as the JCRF, to provide an advertised pathway to bring in industry expertise alongside military service for this specific capability.

Beyond research, the **MOD needs to clarify its strategy for exploitation** of sovereign capability and improve collaboration between industry and key stakeholders. Current goals for exploitation and adoption are unclear and it is essential this is refined to ensure success. Innovation will likely come from a variety of nations and unless MOD supports local innovation it risks being leapfrogged by investment overseas.

BT is driven by an ethical approach to AI, as such we see a need to ensure that there is adequate testing, validation and verification of the technology from conception through life. This is an area where government and industry alike need to put significant resource.

We are reassured by the MOD's promise in the 2022 Defence AI Strategy to "be transparent about the ways in which we are using AI" and believe it is crucial for **building public confidence** and enabling private industry to work together to utilise the technology responsibly.

The MOD should also consider the key enablers of AI. The Defence Digital Strategy was released in 2021 with a target of 2030, but continuing and more **ambitious transformation is necessary** to ensure the availability of key data if AI is to be utilised effectively. Use of AI is still nascent with capabilities and requirements changing at a rapid pace and transformation programmes need to be suitably ambitious and delivery leads appropriately empowered. In particular, the recent developments within the field of generative AI have changed the trends for future capability. We should adapt accordingly.

There are a number of key areas where we feel MOD's strategy would benefit from further attention:

- Long-term collaborative partnerships with industry and academia to ensure sovereign capacity
- Acceleration of fundamental research to higher technology readiness levels to enable Defence to exploit novel AI at pace
- Identification of key AI vulnerabilities and risks across its landscape
- The development of common platforms and networks for international collaboration (e.g., AUKUS)
- Monitoring progress of MOD's digital and data strategies and their applicability to current AI trends

In conclusion, we are supportive of MOD's strategy for AI and the role they see for British industry. However, we must emphasise that in order for MOD to stay ahead in the competitive world of AI it needs to **work closely with strategic partners, facilitate relationships with key stakeholders and invest in large scale innovation and exploitation** programmes. The published strategies are clear and encouraging but need to be ambitious in delivery of key goals if it is to adopt AI at the necessary pace.

We welcome engagement with the Government to provide a deeper level of evidence and discussion, to work together and navigate the challenges and opportunities that AI brings for UK Defence.

8th February 2024