Written evidence submitted by Dr Mikolaj Firlej.

My name is Dr Mikolaj Firlej (https://www.surrey.ac.uk/people/mikolaj-firlej) and I am delighted to submit my evidence for a Sub-Committee on Developing AI Capacity and Expertise in UK Defence as I believe that both my professional and academic experience could support a policy process in this area.

I have been working in the field of AI policy in defence since 2016. I am an Assistant Professor at the AI Institute, University of Surrey where I am leading a research portfolio in the field of AI in security and defence from a policy and regulatory perspective. I have been awarded a DPhil at Oxford's School of Law for a thesis investigating the US Department of Defense policy on Autonomous Weapon Systems.

In addition to my academic work, I have invested - as a co-founder of Expeditions Fund - in several defence and dual use startups in the UK, Europe, and US, including novel threat intelligence solutions and AI security and safety startups.

See below my comments:

1) **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?**

The UK MOD has clearly stated its priorities in Defence Artificial Intelligence Strategy, published in 2022, and the introduction of the Defence AI and Autonomy Unit (DAU) and the Defence AI Centre (DAIC). However, more legal and operational work is required in translating these priorities into tangible outputs.

While I agree with the priority outcomes set out in the Strategy (2022), I believe that the key application of AI should be in faster processing of OODA loops (observe, orient, decide, act) to gain decision advantage over adversaries and, ultimately, leading to the applied autonomy for command and control (C2) systems. In this context, it is necessary to have a legal and operational clarity over the scope of the use of AI-enabled autonomy for targeting and lethal engagement purposes. The MOD has set out, including in the 'Ambitious, Safe, Responsible' policy that UK Defence does not possess and does not intend to develop fully autonomous weapon systems (AWS). Such a statement is not helpful given that certain types of AWS can be not only useful but also preferable than other weapon systems (note, e.g. that not all of AWS can be used for lethal purposes). In the UK policy, one can read that 'the use of such weapons could not satisfy fundamental principles of International Humanitarian Law, nor our own values and standards as expressed in our AI Ethical Principles'.[1] Again this statement is not true, even for some lethal engagements. A lack of clear regulatory framework which could help to assess the scope and use of AI-enabled autonomy in weapon systems is surprising as the UK MOD is pursuing more than 200 AI projects to develop lethal weapons systems, including drone swarms.[2] Further, in the UK MOD Strategy (2022) one of the listed AI opportunities

[1] UK MoD, 'Ambitious, Safe, Responsible. Our approach to the delivery of AI-enabled capability in Defence. ANNEX C: Lethal Autonomous Weapon Systems (LAWS)' (June 2022).
[2] Peter Burt and Chris Cole, MoD AI projects list shows UK is developing technology that allows autonomous

are autonomous, ‘uncrewed adjuncts’. Such systems have already played a critical role in the Ukraine war while the UK MOD lags behind other countries in developing small, affordable, autonomous systems.

As a second area of focus, I would prioritise using AI to unlock new capabilities, e.g. as a co-pilot for exploiting new vulnerabilities, generate new attack plans, or sensitive data extraction. However, the exploitation of new opportunities for defence requires a closer and more efficient engagement with early-stage tech companies which are often at the forefront of AI development. However, the UK MOD procurement process is slow, lengthy, and complex. Early-stage companies do not have enough resources or the ability to bid due to short runways. While the UK Government has introduced several promising initiatives to tackle this problem, such as National Security Strategic Investment Fund (NSSIF), Defence Innovation Fund (DIF) and Defence and Security Accelerator (DASA), the adoption of AI applications developed by early-stage tech companies is still limited across the UK Armed Forces.

Finally, there is limited publicly available information about the potential successes of introduced initiatives. For example, DASA has a small budget of around £50m and, so far, the
biggest beneficiaries are large prime contractors such as Thales or BAE Systems, rather than early-stage defence-tech companies. Very few defence-tech companies, if any, have started out with DASA grants and gone on to achieve a larger commercial scale. NSSIF was created over 5 years ago, but besides some case studies, there are limited information about the potential strategic return on investment of such vehicle for the defence and intelligence community in the UK, let alone for the wider government.

2) **What strengths and expertise does UK industry currently have in the field of Artificial Intelligence with defence applications**

The UK has a wide pool of AI talent, strong research centres and thriving AI early-stage companies. The UK has likely the most vibrant defence-tech ecosystem across all European countries and there are several promising British defence-tech companies already generating millions in revenue in areas such as global threat intelligence, signal intelligence, edge simulation for training purposes or the management of human networks at scale. There are also several British emerging defence and dual use funds, but generally this sector is underinvested with just few experienced fund managers managing micro-VC funds capable at leading rounds from pre-seed to, at a maximum, smaller Series A. As a result, successful dual use and future defence-tech companies originating from the UK must seek growth funding opportunities in other countries, notably in the US.

While the UK has strong human resources in AI and several promising defence-tech companies, my professional experience shows that the government is generally slow with implementing and adopting innovative AI products, particularly within the defence industry.[3] This is somehow reflected by the recent Global AI Index created by UK news company Tortoise. The UK ranked at least tenth in all areas of the

---

drones to kill (2023): https://dronewars.net/2023/07/29/mod-ai-projects-list/

[3] A notable exception is a directorate of the UK Special Forces which is generally a faster adopter of innovative capabilities in the British Armed Forces.

investment and innovation pillars and even higher in talent and research. However, in infrastructure the UK ranked 24th out of 62 and in operating environment just 40th.[4] Similarly, according to influential Oxford Insights AI Readiness Index, the UK achieved 3rd position globally, but scored poorly in AI adaptability.[5]

3) **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?**

First of all, many software engineers are reluctant to work on defence-oriented projects, so it is essential to create structured ways to convey them a message that working in the national security community could be rewarding and filled with hard, intellectually stimulating problems to solve. A good example of such initiative, albeit at a relatively small scale, is a program Hacking for Defense,[6] which is a university course sponsored by the defense departments that teaches students to work with the defense and intelligence communities to rapidly address the nation's emerging threats and security challenges. Further, the Government could consider creating smart match-making program to allow veterans and professionals from defence and intelligence sectors connect with top AI engineers interested in national security. There are several successful commercial matchmaking programs such as Entrepreneur First, so the government could use some of existing best practices, rather than building from scratch. Finally, the government could consider a 'sandbox environment' for high-risk experimental uses of advanced AI, including generative AI, that is accessible to both members of the UK Armed Forces, private companies, and engineers.

18th January 2024

[4] https://www.tortoisemedia.com/intelligence/global-ai/
[5] https://oxfordinsights.com/ai-readiness/ai-readiness-index/
[6] https://www.h4d.us/