Andrew Otterbacher, Director, Scale AI – Written Evidence (AIW0043)

1. Do you think that there is sufficient sharing of information relating to AI between the US, UK, and other allies, including data-sharing? Is this data of sufficient quality? What is most often missing and why?

The concept I often refer to as the "AI Triad" comprises Compute, Data, and Talent. Focusing on the Data aspect, particularly its quality, reveals that the challenge isn't the volume or frequency of data being shared between the US, UK, and allies, but extracting actionable insights that can be derived from this data. Policymakers are not simply seeking more data; they require insights that are immediately usable to improve decision calculus.

By "usable," I mean data that meets several quality criteria: it must be relevant to the policy questions at hand, accurate in its measurements or assessments, complete in its scope, consistent over time, and well-labeled for immediate ingestion into AI algorithms. Unfortunately, most incoming data falls short of these standards, incoming petabytes are piled on top of previously collected exabytes which in turn are piled on top of zettabytes. To put the scale into perspective, just one small unit of one branch of the US armed services generates over 20 terabytes of data daily. Yet, much of this massive amount of data remains untapped, leaving one uncertain whether the collected data was even relevant to, or effective in, assisting policy judgements.

For the US, UK, and other allies to maintain a leading edge in AI, it is critical not just to share data, but to curate and exchange "AI-ready" data that can be immediately used to extract meaningful insights. Future efforts should focus not just on the amount of data being shared, but on improving its quality to make it instantly actionable for decision-making processes.

2. How should the US and UK take forward and operationalise the draft articles they submitted at the CCW?

To effectively take forward and operationalize the draft articles submitted at the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (CCW), the United States and United Kingdom can draw valuable parallels from the Department of Defense Directive 3000.09 on "Autonomy in Weapons Systems," which was codified earlier this year. Both sets of guidelines tackle comparable ethical, legal, and operational issues around autonomous weapons systems (AWS).

1. Training: To ensure comprehensive understanding and responsible usage of AI-powered weaponry, specialized training programs need to be established. These courses should be designed for both service members and commanders, covering the ethical ramifications, technological capabilities, and strategic applications of AWS. Adequate training will create a foundation upon which AI and AWS can be more effectively and ethically integrated into military operations. Our experience shows Commanders need training on how to implement AI into the decision-making workflow chain and should schedule multiple practical exercises beginning with Command and Staff tabletop exercises to full Field Training Exercises than incorporate AI enhanced decision-making tools and weapon systems.

2. Development of TTPs (Tactics, Techniques, and Procedures): Clear TTPs need to be developed to ensure uniformity and efficacy in the use of AWS. This would include best practices for deployment, escalation of force, and decision-making hierarchies, among other operational considerations. TTPs serve as a practical guide for both commanders and operators in the field, helping to standardize procedures and mitigate risks.

3. Doctrine Formation: Lastly, the training modules and TTPs should be integrated into a broader doctrinal framework. This allows for a more structured approach to implementing AWS and provides a formal platform for periodic review and updating. This evolving doctrine would serve as a comprehensive guide for understanding the function, capabilities, and limitations of AWS under realistic operational conditions.

In summary, the next steps for the U.S. and the U.K. should focus on the rapid yet responsible operationalization of the draft articles from the CCW. This entails developing rigorous training programs, formalizing TTPs, and establishing an encompassing doctrine that is aligned with existing guidelines so we can ensure that the integration of AI and AWS into military operations is done in a manner that is both effective and ethical.

□

3. How effective do you consider export controls around hardware used in AI, such as semiconductors?

Export controls on hardware components like GPU (graphical processing unit) and HBM (high bandwidth memory) are a critical but complex facet of national security, technology leadership, and international diplomacy. On one hand, these controls are essential for preventing the misuse of advanced AI technologies, especially in areas that have ethical or defense implications. Limiting the export of critical hardware components to certain nations or

organizations can slow the rate of development of advanced AI systems. On the other hand, the effectiveness of such export controls is determined more by the will of the targeted country to either build alternative supply chains (e.g.; Iran, DPRK), or to focus capital and labor to replicate the components internally.

Per the South China Morning Post, "While it will be an uphill battle to catch up with global leaders like SK Hynix, Samsung Electronics, and Micron Technology given the impact of Washington's sanctions, the Chinese government has determined that the country must become self-sufficient in HBMs even though it may take years." In fact, many Chinese firms have been stockpiling NVIDIA GPUs over the last year as well as placing upwards of $5 billion dollars of orders in advance to cushion expected export controls. Such measures could allow countries to bridge the gap between the export controls and the development of an indigenous capability.

In addition, other challenges exist:

1. Technological Advancements: The rapid pace of innovation in AI and hardware can often outpace the legal and regulatory frameworks in place for export controls, necessitating constant updates and revisions to remain effective.
2. Collateral Limitations: The controls also have an impact on international collaborations in research and development, sometimes causing delays or cancellations of multinational projects that could otherwise benefit global progress in AI.

In summary, while export controls are a necessary tool for mitigating risks associated with the global distribution of AI-related hardware, their effectiveness is a complex equation balanced between security concerns, innovation, and international cooperation. Striking this balance demands continuous evaluation and adjustment of existing policies to adapt to the fast-paced evolution of technology and geopolitical considerations – an area on which I believe the UK, the US, and allies should be increasing cooperation and information sharing.

Andrew Otterbacher
Scale AI
October 2023