Written evidence submitted by Rebellion Defence

About Rebellion Defence

Rebellion Defence brings together world-class technology talent with deep national security expertise. We build advanced software exclusively for the mission of national security and defence. In partnership with our customers, we're building critical foundations for the digital backbone that underpins UK defence and security: powering data analysis from the cloud to the tactical edge, keeping data and weapons platforms secure, and transporting data at machine speed across classifications and allies.

The collection, use and analysis of data across national security relevant departments, and the mechanism for the NSC collecting evidence to aid its decision-making.

The United Kingdom's position as a leader in national security and technology hinges on our approach to data and decision making. As we rethink the meaning of "Global Britain" in the period post-Brexit and post-Pandemic, we must also rethink our approach to data and decision making. The focus of our submission is on the collection, use and analysis of data across national security relevant departments and the mechanism for the NSC collecting evidence to aid its decision making. The key to unlocking the potential of the data at our fingertips is to **bring together human expertise with technology to make better decisions from data**.

To achieve this, we need **technological**, **behavioural** and **organisational** change. We must invest in the best technology and architecture to connect and transform data, build institutional knowledge, and inform decision making. Government should also implement rules, frameworks and new legislation to promote necessary behavioural and organisational change across Whitehall.

Summary of Evidence:

- Government has vast amounts of data at its fingertips, but data exists in siloes. We need to **connect data and remove siloes** to make it useful. Data must be **situated in full context** to derive insight and inform decision making. Government can use tools, such as knowledge graphs, to show the links between data sets and to situate data in full context. **Centralising data**, or making it widely and instantly accessible across government, would make it easier to contextualise and analyse, and increase the likelihood that data is used to influence strategy and decisions.

- The **speed of information transfer** is a critical precondition for effective decisions.

- Government often relies on imperfect data sets that are the product of inefficient or biased processes. We need the **best data sources**, as well as the right technologies and better data architectures, to benefit from the analytical observations possible from our data. The call for evidence refers to collecting, using, and analysing data from across 'National security and relevant departments.' How does the Government define a "relevant" department? To get "good" data, it is vital that governments embrace a **wide and diverse selection of data inputs** that it typically would discount as being "irrelevant". Moreover, Government should not be overconfident that it has "good" data; we must always question assumed knowledge. The data we use to build knowledge and understanding is constantly evolving. Data sources can be like assumptions and must be challenged and updated as we are confronted by new data and experiences.

- Artificial Intelligence and Machine Learning need careful **training and testing** in order to be useful. They are only as good as the data used to train them.

- **Humans must always be at the heart of decision making.** In putting machines to use doing what they do best, we **free the human mind** for imagining creative solutions to complex national security problems.

- Data must be presented in a **clear and accessible format** so that it can inform decisions. It should not be too complex for human decision makers to understand. The role of the machine will often be to simplify, categorise, group, and reduce the amount of information shown to people.

- **We will not make good decisions simply because we have the right - and clearly presented - information.** Technologies must be enabled by **behavioural and organisational change**. Government needs to build and implement programmes to demonstrate and realise the value of data, (e.g. Government could incentivise and empower data custodians to 'unlock' data's potential by making it accessible to data scientists and decision makers.)

- Building **public trust** is crucial if the Government wants to access personal data in the same way that third parties in the private sector can, and already do (e.g. to Private Health Insurance, Mortgages Brokers etc.).

- To realise the value of, and gain access to, data we need **new legislation** that provides enough flexibility to keep pace with technological change.

How we can help:

Rebellion Defence believes that the United Kingdom needs the best technology, built by the best engineering talent, to protect a rules-based international system that allows democracy and humanitarian values to flourish across the world. Modern wars have become a battle for information, in which state and nonstate actors weaponise information and data. Our adversaries leverage cutting-edge technologies against us and indiscriminately abuse the open internet. For the UK and its allies to bolster their presence in an ever-changing digital environment, we must harness the very best analytical capabilities. These capabilities must accelerate the UK and its allies' information advantage against our adversaries. To do this will not only require deep synthesis and analysis of Authority-derived data, but, more critically, a persistent and rapid acquisition of multiple publicly available sources of information and data.

Rebellion Defence is developing an integrated suite of solutions specifically designed to enhance the command decision process and aid effective decision making. Our solutions provide near-real-time data extraction and analysis, employing continuous vulnerability identification and prioritisation to ensure the networks that data are secure, and ensure that information is safely transported across systems and security levels. Moreover, our products are purpose built to scale a spectrum of use cases. The modular design, open architecture, and rapid ingestion, transformation, and normalisation pipeline ensure that they are adaptable and scalable, and eliminate silos.

Rebellion ANALYZE

Using artificial intelligence/machine learning (AI/ML) capabilities, Rebellion Defence automates the science of turning sensor data into mission-critical information, freeing analysts to do the art of intelligence.

Rebellion's ANALYZE drives actionable insights from high-volume of data at an order of magnitude faster than existing solutions. ANALYZE creates a common analysis platform for users across a shared mission to interact with data and collaborate on user-defined priorities. Our AI algorithms continuously monitor and uncover connections from data as they are ingested in real-time, freeing users from manual data analysis to focus on mission planning.

Below are brief descriptions of capabilities within this product line that Rebellion is currently addressing:

(I) Command and Control

It is not uncommon for analysts to labour over massive varieties and quantities of data using tools such as spreadsheets and slideshows. This means they can only consider a fraction of the data collected before a data set becomes obsolete. When transporting data across domains, they

may be forced to turn to manual processes to share information with colleagues. These manual processes sit at odds with the need to understand what is happening, make intelligent decisions, and turn those decisions into action, all in near-real time.

As the threats of great power competition become clear, Rebellion Defence provides AI-enabled capabilities that accelerate how those charged with national security and defence understand, decide, and act. Traditional chains of command are linear in nature, and consequently create time-consuming processes in the decision-making chain that can be costly in terms of resources and lives. Rebellion Defence's AI/ML-driven data analysis software, not only enhances the data analysis function but also enables more dynamic, lateral command-and-control networks, with greater delegation of authority, allowing exploitation of relevant information at speed. Rebellion Defence's cross-domain solutions increase speed from data collection to decision by facilitating seamless data sharing across networks and security levels, further enhancing the command-and-control process.

(II) Multi-Domain Expertise

Today's vast array of sensor types provide massive amounts and varieties of data to national security and defence agencies; however, harnessing intelligence from these data sources presents unique challenges for interpreting the often niche data they produce.

Commercially transferrable AI capabilities to exploit niche data do not exist due to expense, access issues, or regulations required to leverage these types of sensors in commercial markets. These data types present usability issues, as their outputs are typically overwhelming, in terms of both quantity and quality. To fully exploit niche data, they must be fused with other intelligence in near-real time and presented to analysts with appropriate context to drive operational insights. These data types can complement each other and augment more traditional intelligence-collection methods, increasing mision-data usability and overall battlespace awareness.

In addition to our work with analysing data from captured exploitable materials and traditional optical sensors, Rebellion Defence also offers software for rapid extraction, ingestion, and processing of publicly available information for augmented investigation and analysis.

(III) Publicly Available Information

Rebellion has developed a machine-learning (ML) powered platform to extract, process, and analyse publicly available information (PAI) in real-time, surfacing mission-critical insights and vulnerabilities for intelligence analysts. This platform helps organisations to better detect emerging events, aggregate and fuse disparate sources, and discern actionable outcomes which prevent the further spread of disinformation.

12 February 2021