VEREDUS TALKS

## *An interview:*
## *Anthony Mensier – Disruptive Industries*

# AI IN DEFENCE

**Stephen Womersley, Director in the Defence, Nuclear, Infrastructure & Technologies practice at Veredus, speaks to Anthony Mensier, Chief Technology Officer at Disruptive Industries about how AI might inform the Defence and National Security ecosystem**

**Today we are talking about AI in defence, but firstly can you give us an overview of Disruptive Industries, recently highlighted in the Telegraph as a AI Start up to watch!**

Disruptive Industries was created by former intelligence officers to address problems they faced in government work. The company specialises in mapping unknown risks through a modular and scalable threat sequencing system. This system can ingest various data feeds, both internal and from customers, and provide intelligence analysts with insights and a full record of the data behind conclusions.

Disruptive Industries differentiates itself by applying a range of computational models and data processing techniques, rather than solely relying on AI, to best solve customer problems. The company focuses on transparency so conclusions are traceable to their original data sources. This approach has gained traction in defence and national security fields where accountability is important, but also in specialised commercial markets such as War Risks Insurance.

**Many have the perception that AI is another "Black Box" -  a technology only really understood by a select few. Can you dispel that perception and explain in layman terms what AI really is?**

AI was described as a broad field of computer science focused on creating systems capable of tasks typically requiring human intelligence. It involves machine learning algorithms that learn from data to provide outputs, as well as deep learning using neural networks as a more complex form of machine learning.

Generative AI differs by creating new content rather than just predicting outputs, such as through large language models that take questions as input and output new text.

**The global race to stay ahead in terms of "AI in military capability" is very much on, where do you see UK defence in that race at present?**

The UK has several key capabilities for frontier AI research applicable to defence. The Alan Turing Institute conducts advanced computing applications across defence, environment, and health domains. It recently opened a new branch for fundamental AI research led by an ex-colleague and friend.

Government initiatives like the Frontier Lab Task Force also aim to keep pace in AI development. While the UK lacks some of the large computer centres needed for models like large language models compared to the US, it has a strong talent pool of data scientists and engineers graduating from universities that can help advance research and production. London, Cambridge and Oxford in particular have a large tech startup and university ecosystem that outputs top talent, positioning the UK well for AI work. It is also home to one of the most famous Frontier Labs  DeepMind, acquired by Google in 2013.

**We have seen how AI can be incorporated into many areas of defence to enhance decision making and increase accuracy of data. Also with the use of drones and autonomous vehicles in mission environment, as well as for complex analytics, threat detection and cyber security. Ukraine has provided a real-time event that has driven AI to new levels. Where do you see the main growth areas for AI in the short- to medium-term?**

Computer vision will see greatly increased accuracy in object detection from images and videos, able to distinguish specific models of vehicles. Mathematical models and swarm technologies will enable increased autonomy and coordination of systems.

Large language models can accelerate the development process by outputting code to solve problems, bringing more people without computer science backgrounds into technology development roles. This aims to increase efficiency rather than replacement. Leaders should consider a variety of advanced data analytics processes and specialised AI models and how to integrate them to best solve problems, rather than relying and focusing solely on the latest technological trend such as the large language models wave.

**The growth of integrating AI will bring about a change in many organisations. To effectively manage and develop AI systems how can today's leaders prepare for this wave of AI technology?**

Leaders must understand available AI capabilities and user problems to define success metrics when adopting AI. This involves having technology teams directly engage with users to fully comprehend problems.

Prototyping aims to solve simple, well-defined problems first before attempting more complex issues. Early successes can be achieved through systems that increase efficiency by automating basic tasks for analysts, like using advanced computer vision for specialised object counting, while still allowing for human verification and oversight. This controlled introduction of AI helps organisations adopt the technology in a practical manner focused on user needs.

**As with any technology there is an ethical side to AI, we constantly see the moral and legal arguments for its use. What's the AI industry doing to allay these concerns?**

Companies developing AI must ensure proper input and output monitoring to build user trust. However, tracing decisions within complex models like deep learning is difficult. Firms should educate users on capabilities, limitations and potential risks to prevent harm from misuse or vulnerable models.

If leaked, generative models trained on sensitive data could enable reverse engineering. Developers bear responsibility for securing models and outcomes of their use.

**When AI is used for strategic decision-making who checks the AI result?**

Defence must, and in some do, carefully tests AI systems before use to ensure they exceed human performance. Multiple checks occur during development, including review by experts and testing in simulated scenarios.

Systems should then be deployed in live training exercises to further evaluate performance. Once confident in a system's abilities, it may be introduced with humans monitoring at all stages. Constant oversight continues after field implementation to maintain safety and effectiveness. Human judgment also factors into final decisions.

**What’s to stop defence becoming over-reliant on AI? How do we keep a balanced approach to its integration?**

Maintaining a balanced approach to AI integration requires understanding where and how AI systems are used within an organisation and their accuracy levels. More accurate systems like automated calculations can be highly relied on, while generative systems may have lower confidence rates that require monitoring and control measures.

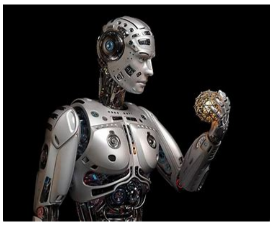
It is important to map all AI deployments, understand their capabilities and limitations, and ensure alternatives are available should systems need to be replaced. People within the organisation must comprehend each system's functions so dependencies can be managed and issues addressed without sole reliance on external parties. Oversight allows assessing overall dependence on AI while mitigating risks from less predictable technologies.

**Are you noticing any business leader bias toward AI? Eg. Fixed firm views you have to counter?**

There is currently a strong pro-AI bias among business leaders, especially in defence. Leaders feel pressure to test and deploy AI widely to prove its adoption. However, technology providers warn that rushing implementations risks forcing AI uses where they may not be needed or ready.

Proper problem definition and prototype testing is advised before deployment to ensure AI solves real problems effectively. Leaders should select use cases strategically based on clear criteria rather than just to demonstrate AI adoption.

**We have all seen Terminator with its Skynet AI foe, how far off do you think we are from a truly autonomous AI system on a global scale?**



Estimates are that within the next 10 years, artificial intelligence systems may surpass human levels of intelligence in specific, narrow domains. However, a generally intelligent system with human-level cognition and self-awareness is still further off. Near-term risks are more likely to arise from how advanced AI is applied by humans, through poorly thought-out instructions, rather than systems becoming autonomously malicious.

Proper governance and oversight are needed to ensure AI is developed and used responsibly, as even very intelligent systems would still take their goals from human programmers and managers. Care must be taken to avoid unintended, harmful consequences that could arise from ambiguous or overly broad instructions given to powerful AI.

**Stephen Womersley**

Director - Defence, Executive Search
Veredus

Stephen.womersley@veredus.co.uk

**Anthony Mensiers**

Chief Technical Officer
Disruptive Technologies

Anthony.mensier@disruptive-industries.io