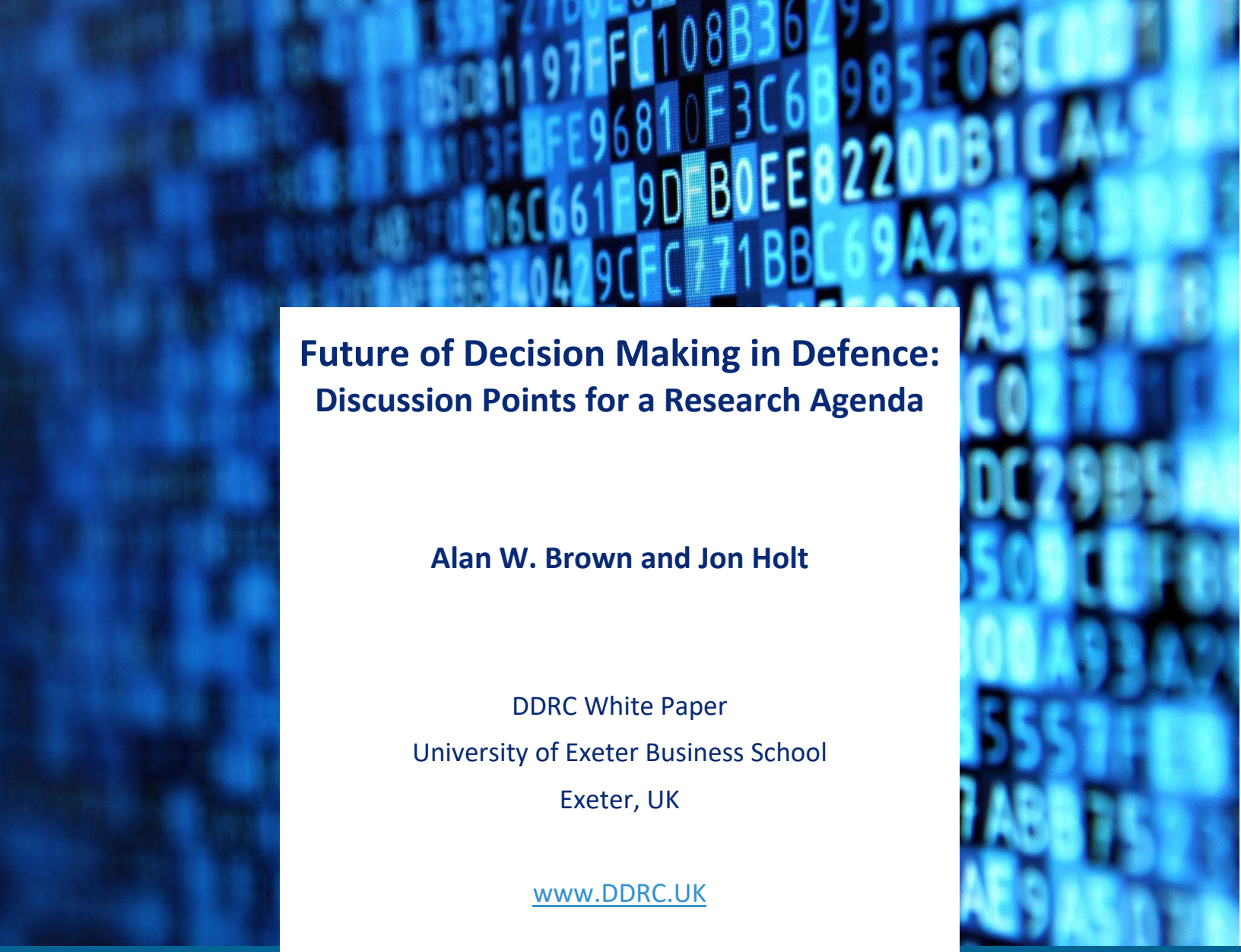

Future of Decision Making in Defence:
Discussion Points for a Research Agenda

Alan W. Brown and Jon Holt

DDRC White Paper

University of Exeter Business School

Exeter, UK

www.DDRC.UK

July 2023

Report number: DDRC – 06/23

DEFENCE DATA RESEARCH CENTRE

Future of Decision Making in Defence

INTRODUCTION

In July 2023 the Defence Data Research Centre (DDRC) hosted an all-day series of meetings to discuss global trends in defence data, and to focus attention on the implications of current digital technology advances for *the future of decision-making* in defence in a world that is increasingly data driven.

We were honoured to bring together guests from:

- **DDRC - including hosts *Zena Wood, Alan Brown* and *Roger Maul.***
- **Defence Science and Technology Laboratory (DSTL) - including keynote speaker: Principal Advisor.**
- **Engineering and Physical Sciences Research Council (EPSRC) - including keynote speaker: Director of Partnerships.**
- **Hoover Institution - represented by keynote speaker: Visiting Fellow.**
- **Gordian Knot Center - represented by keynote speaker: Assistant Director.**
- **Central Intelligence Agency (CIA) - represented by keynote speaker: CTO.**
- **Defence AI Centre (DAIC).**
- **Royal Air Force (RAF).**
- **Alan Turing Institute.**
- **Defence industry and data strategy experts.**

This report highlights the main themes and concepts discussed at these events. A wide collection of perspectives and views were presented with many distinct positions being outlined on these important topics. Hence, this report focuses on outlining the variety of voices from the audience and placing them in context with the aim of exposing a range of potential directions for future research. In particular, as an open set of discussions, this report explicitly avoids direct reference to individual statements and opinions.

CONTEXT

DDRC is undertaking a 3-year research programme bringing together expertise in data science, computer science, and social science to improve the use of data in the defence community. Its work is funded by the Defence Science Technology Laboratory (Dstl) in support of the broad digital transformation taking place across the UK defence sector. The specific role of DDRC is a response to the UK Digital Defence Strategy which states that by 2030 "our understanding of national and local risks will be dynamic, driven by data and insight where appropriate, and informed by the best UK and international expertise and experience".

As part of its mission to research problems related to the use of data for artificial intelligence applications, DDRC is looking to strengthen ties with prominent academic organisations and leading Defence institutions worldwide. The meetings forming the basis of this report represent the first in a series of planned exchanges with counterparts overseas to align and share knowledge on a variety of topics on data science and AI in defence. This initial focus was on the future of decision-making in defence in times of digital transformation and the need for international cooperation amongst allies, considering the near term demands (1-5 years), medium term opportunities (5-10 years), and future implications (out to 50 years).

The DDRC is now seeking to cement relationships with these leading research units with the aim of sharing insights and accelerating progress for the benefit of our respective Defence organisations and the safety of our nations. We were encouraged by the collegiate nature of this initial event and outstanding inputs, and look forward to working closely on joint outcomes.

BACKGROUND

Over the past decade we have seen significant advances in digital technologies to improve their capabilities, extend their capacity, decrease their costs of production, and expand their application. As a result, we have seen major steps being taken in their adoption in every aspect of business and society. As experiments and early adoption of these technologies has accelerated, not only have organisations begun to recognise the broad impacts they will have on future strategies, they also are beginning to transform fundamental concepts that define the core of their operational approach.

In the defence sector, digital transformation has been particularly important. From incremental improvements to defence equipment procurement processes to the disruptive impact on the nature of warfare, digital technologies have demanded a deep reassessment of every aspect of how to move forward. This has immediate implications. Ongoing conflicts, such as those in Ukraine, have highlighted in real terms how attitudes and actions to digital technology adoption influence many aspects of defence strategy and tactics.

The scale of investment in defence is worth noting. The defence sector is a critical aspect of UK infrastructure and a major part of the UK economy. In 2020/21 the UK government spent over £40 Billion on defence, including over £1 Billion on research activities. In addition, the UK defence industry turnover was approximately £25 Billion with over £10 Billion in exports. When combined with associated industries such as aerospace, the defence sector contribution to the UK is very significant and highly influential. Over coming

years, the effects of digital transformation on defence **will have important implications** for why, how, and where this budget is spent.

AI in Defence

Given this context, it is no surprise to see that Data Science and Artificial Intelligence (AI) feature highly in the UK's future defence plans. Released in July 2022, the UK **Defence AI Strategy** offers an important insight into the opportunities and challenges of AI in this sector. These were elaborated in **a policy statement released with this strategy** in which the UK MoD outlined a number of principles on which the use and adoption of AI would take place in this sector.

Fundamental to its approach, the UK MoD highlighted the challenges of realising the benefits of AI across its domain. In particular, it emphasised that it saw the digital transformation of the UK defence capability to be one of the most critical strategic challenges of our time. While equipment and supply chains will require digitisation, the UK MoD recognises that a more fundamental change is required to adjust to the digital era. The goal, **according to the policy statement,** is "to adopt and exploit AI at pace and scale, transforming Defence into an 'AI ready' organisation and delivering cutting-edge capability".

The challenge, it recognised, is how to achieve this goal in a diverse, complex organisation involved in a wide range of intense activities across the world. Furthermore, it is a challenge made even more difficult with the disruptive nature of AI and the consequence of its use in decision making where lives and livelihoods are at stake. A difficulty that was clearly identified in the policy statement:

"…the issue may not lie in 'what' the capability is designed to do, but 'how' it does it, and how we ensure that AI is used effectively and appropriately."

Digital Impact on Decision Making

Nowhere is the disruption of data science and AI more significant than in how decisions are made in situations of uncertainty. The future of decision-making for leaders and strategists in the defence sector with the increasing use of digital forms of warfare is expected to be heavily influenced by advancements in technology and data analytics. New data sources and high-speed intelligence analysis bring new opportunities to influence human decision making and automate much of the decision-making process. However, inevitably the rapid evolution of digital technology raises new questions about the limits of digital warfare and introduces a wider range of cyber threats. Consequently, decision-making processes will need to adapt to meet these new challenges effectively. Several trends and developments will shape the future of decision-making in the defence sector, including:

Data-Driven Decision Making: With the increasing interconnectedness and digitalisation of defence systems, leaders and strategists will have access to a vast amount of data from various sources. Analysing and interpreting this data will become crucial for decision-making. Advanced data analytics, artificial intelligence, and machine learning will be employed to process this information rapidly and provide actionable insights.

Cybersecurity and Resilience: As digital warfare becomes more prevalent, decision-makers will need to prioritise cybersecurity and resilience as fundamental components of their strategies. Protecting critical infrastructure and sensitive information from cyber threats will be paramount, and leaders will need to develop strategies that integrate cybersecurity into every aspect of defence operations.

Real-time Situational Awareness: The increasing use of digital technologies will enable real-time monitoring and situational awareness. Decision-makers will have access to live data streams, enabling them to respond quickly to emerging threats and changes on the battlefield. This will require the ability to process and understand data in real-time, making agile decision-making essential.

Human-Machine Interaction: As advanced technologies like artificial intelligence, autonomous systems, and drones become more prevalent, decision-makers will need to embrace the concept of human-machine teaming. Leaders will rely on machines to assist in data analysis, simulation, and predictive modelling, while human intuition, creativity, and strategic thinking will continue to play a critical role in decision-making.

Simulation and War Gaming: Given the complexity and risks associated with digital forms of warfare, leaders and strategists may increasingly turn to advanced simulation and war gaming exercises. These tools can help decision-makers test various scenarios, evaluate potential outcomes, and identify vulnerabilities in their strategies without real-world consequences.

Collaboration and Partnerships: With digital warfare being a global challenge, collaboration and partnerships between different defence organizations, allied nations, and private sector experts will be essential. Decision-makers will need to be adept at fostering collaboration and information-sharing to stay ahead of rapidly evolving threats.

Ethical Considerations: The use of digital technologies in warfare raises ethical questions about accountability, transparency, and the potential for unintended consequences. Decision-makers will need to carefully consider these ethical dimensions in their strategies and decision-making processes.

Investment in Training and Education: To navigate the complexities of digital warfare and make informed decisions, defence leaders and strategists will need specialised training and education. Continuous learning and staying updated on technological advancements will be crucial.

These current considerations are strongly influencing the discussions taking place today on the future of decision making in defence. However, it is essential to recognise that digital technology and the nature of warfare are continually evolving, and the future of decision-making in the defence sector may bring about new challenges and opportunities. Therefore, leaders and strategists must remain adaptable and proactive in

their approach to decision-making while staying informed about the latest developments in digital forms of warfare.

SUMMARY OF DISCUSSIONS

Seen in this context, the discussions that were held in July 2023 address a number of core concerns and highlight several potential directions for future research. These are summarised under five key headings.

Organisational models, and the future of warfighting

- **We discussed the history of warfighting, and the accepted models of armed forces organisation and decision making. The *de facto* - Napoleonic - model of command/central staff dominates armed forces. *'The staff is the analogue tool that gives information to a commander, who makes a decision'.***
- **We are moving from a hardware-centric model to software-driven improvement, arguing that rapid iteration (impossible with hardware-centric models) will keep costs down and maximise effectiveness. The DOD behaves, essentially, 'like a hardware company in the 1980s'; this needs to change - and the group pointed to a paper of 2022: Software defined Warfare (Mulchandani & Shanahan) *'The only way for the DOD to remain competitive in this new warfighting environment is to ensure that it uses the most potent weapon available; technology, and more specifically, software'.***
- **In terms of long-term goals, Defence leaders can struggle to comprehend the 50-year goal (fantastical 'computer plugged into brain'-type advancements) and may respond better to looking at iterative improvements that will yield iterative improvements. In any case, as Defence catches up with modern tech, it has much to assimilate in even the 'state of the practice' - let alone 'state of the art'.**
- **Existential inversion from 'physical to virtual' in warfighting was discussed, with the impression held by some that it is inevitable that virtual conflict will subordinate physical engagement - invoking proof points from Ukraine and beyond.**
- **Morality and ethics in automated warfare models were discussed in brief, with a suggestion that we must be circumspect - and potentially alter how we discuss the matter; *'it is not just the drone - the automated component - that is under question; it is the whole system'.***
- **Modern warfare - citing Ukraine - is 'like WW1 meets terminator'; drones flying overhead one minute, bayonets in flooded trenches the next'. Such is the state of transition, the 'model' needs to factor in old and new. A historical analogue here is the Spanish Civil War - with its then-innovative combined arms warfare. We might learn from this; if the old military imperative is to impose order on the battlefield, perhaps today we should look to impose 'adaptation' on the battlefield. 'Those who adapt fastest will win', shown to be valid looking at past theatres of conflict where the adaptive army beat an enemy with greater scale and resources.**

- **Supply chains have been newly exposed as a vulnerability (and a proxy target in war?).-Resilience of supply chains is now a major focus for new digital solutions.**

Technology advances in Defence

- **Different areas of Defence have their own constraints; for example, intelligence can move more quickly into AI and future tech, as it lacks the vast scale and hardware-reliance of military operations.**
- **Technology is 'flattening the hierarchical structures of Defence around the world'.**
- **Major change management in AI and data improvement - looking at swingeing institutional resets of Defence organisations - presents its problems. Progress in AI and data is more likely to come from tactical improvements rolled out and rolled up.**
- **Forecasting data-enabled changes to warfighting is only accurate in the short-to-medium term: *'We have a good idea of what things look like in five years; we have a vague idea of what might be available in 10 years; in 30 years, we really have no idea'*. We have to be realistic and agile - yet *prepare* the command for longer-term change, and *imagine* future changes that are beyond current recognition.**
- **DOD *et al* are, effectively, still organised and managed around major hardware procurements and deployments. This not only impacts the delivery and deployment cycles, it also pervades the thinking about strategy, tactics, and operations.**
- **Defence - noted as slow to develop and iterate in cutting-edge technologies - is ironically the origin of 'agile' development. Tactical warfighting battles *force* participants to iterate and evolve when faced by an ultimate price for failure.**
- **We must ensure we are looking for solutions to problems (rather than problems to fit our solutions - borrowing from a venture capital maxim).**
- **We need to be quicker in moving from research to development, putting concepts into laboratories and into the field. This is where academic partners can help.**
- **Social and educational constraints were discussed; in the UK, 25% children are below the threshold of data and digital literacy (with the implication that this statistic is relevant in Defence recruits, likely to greatly dampen progress).**
- **We need to see CTO roles move onto the main board in Defence organisations, otherwise we will not see the right decisions being made.**

Collaboration between nations

- **Emerging tensions - such as in the South China Sea - call for ever-greater collaboration between allies, including via Five Eyes (intelligence alliance of United States, United Kingdom, Canada, Australia and New Zealand).**
- **A proposition on the table is that we formalise university collaboration in a tripartite format between UK-US-Australia, which maps well across military strategic alliances.**
- **Collaboration must be focused on action, rather than conversation. Let us work on real challenges.**
- **Further, investment must be matched - and promises kept - to ensure progress and build trust across partners.**
- **The US (agencies and DOD) are collaborative by nature, but can on occasion assume that ally nations will follow its lead. It needs to see commitments and value if programmes originate overseas.**

Procurement and partnering

- **The natural monopoly state of Defence organisations was discussed, and held up as a major reason for relatively slow progress in technology advancement.**
- **'We need to be a good customer', was an observation - against a backdrop of imperfect relationships with suppliers, and procurement decisions that can become expensive over time; *'a wrench can end up costing a million dollars if it's maintained against a service contract for thirty years'.***
- **IP protection in partnering is not necessarily a problem, as most algorithms are open source. However, we have a tendency to invest heavily in early stage technologies, only to cede dominance by selling our assets overseas before commercial development.**
- **We need to watch state-of-the-art developments in sectors outside Defence, and assimilate progress for our own requirements. Defence processes and solutions have a tendency to be too insular.**
- **We are big and we are slow, when it comes to procurement. Smoothing the relationship between supply and demand is critical. Suppliers often struggle with late payments and opaque briefs.**
- **Small businesses - where so many of the best tech brains reside - find selling to Defence organisations burdensome; how can we better build mutually-beneficial relationships that incentivise more small innovative companies to work in the defence sector?**
- **Government has often 'fallen asleep' on procurement and partnering. They need to be held to account by Defence organisations, and give us the tools we need to buy faster and smarter.**
- **Budgets are so large in Defence that sub-$1bn spends often are viewed as below the radar and do not get the right level of scrutiny - and that is where the interesting software-enabled change is emerging.**

- **Procurement people need to be brought into discussions as early as possible, and helped to understand risks and benefits of a programme from the outset.**

SUMMARY OF DEFENCE AND ACADEMIC ORGANISATION PRIORITIES

Digital transformation presents many opportunities and challenges in reimagining decision making in times of uncertainty. However, it also demands a strong cross-disciplinary perspective to move forward in addressing these needs. Key considerations include:

- **Academia, industry, government - a potentially powerful triumvirate.**
- **Who is driving it forward? 'This should not be just about having clever ideas and observations; it must involve actively implementing and developing them'.**
- **There is no silver bullet, we need to put in the hard work together. The only way to succeed is to *'get in the boat and start rowing'.***
- **Consider in our work the 'leveraged business model'; how can our work have a multiplier effect, so that we can see a logarithmic success trajectory?**
- **Focus on our own challenges - rather than fixating on the manoeuvres of bad actors and potential enemies of our nations.**

To carry out the hard work required to address these topics will demand an alliance across teams with a wide variety of experiences, perspectives, and skills. The following organisations have already expressed their commitment to face up to this challenge:

DDRC is looking to establish itself as a leading international Defence research facility, and is building collaborative relationships with peer organisations. Its goals are research, problem-solving for Defence organisations, impact acceleration in emerging technical areas, broad-reaching education, and community building. DDRC is looking to address each opportunity against risk, trust and value for the Defence community.

DSTL is working on several fronts to improve AI and data science capabilities across UK Defence. It is midway through a sophisticated AI programme, skilling up to meet the challenges of the state. Key tenets of the programme include:

- **Improving reactive intelligence, surveillance, and reconnaissance using best in class technology**
- **Building a cloud/edge compute platform with vendor partners**
- **Extending usage of machine-assisted intelligence gathering**
- **Quantum information processing**

The Engineering and Physical Sciences Research Council (EPSRC) has £8bn to invest in science and innovation, and Defence is a growing area of its strategy. It is working with organisations to find emerging areas which could enable the UK to achieve world-class status. Beyond its large-scale, programmatic work - EPSRC is behind quick-to-fund 'sandpits', smaller research teams that can deploy quickly and get to value straight away. Whilst UK-focused, the EPSRC has Memorandum of Understanding (MOU) agreements with certain ally nations - including the USA, and is looking at National Science Foundation (NSF) co-funding. Indeed, c40% of the EPSRC portfolio has international investment partners.

The Hoover Institution is looking for the investment and buy-in required to allow government/industry/academia to work over a three year period to study emerging trends, and help Defence organisations scrutinise, test and develop future tech and data options. The mooted programme consists of

- **Commissioning original research**
- **Developing feasible, suitable and acceptable future decision-making models**
- **Testing new models via simulation against a baseline of research**
- **Partnering with businesses which may be advanced in a certain area**

The Gordian Knot Center has pioneered a unique model for problem solving in Defence; teams of graduate students work on key (unclassified) challenges faced by the US military. Using semi-structured research methodologies, they study primary and secondary sources covering issues at hand, and test hypotheses in interviews with Defence experts. The problem is reframed against the arguments tested, and reported back.

TAKING THE NEXT STEPS

The result of our initial discussions on the theme of decision making under uncertainty in defence has highlighted several emerging principles that we believe will be central to future activities in this area:

1. **Ensure Cross-Disciplinary Collaboration: Foster collaboration between academia, industry, and government organisations to create a powerful collaborative team. Establish alliances with a wide variety of experiences, perspectives, and skills to address the challenges of digital transformation in defence decision-making effectively.**
2. **Focus on Agile and Adaptable Practices: Embrace agile decision-making processes that can rapidly iterate and evolve in response to technological advancements and emerging threats. Stay informed about state-of-the-art developments in sectors outside Defence and assimilate progress for the benefit of your respective Defence organisations.**
3. **Drive Real-time Data-Driven Decision Making: Leverage the potential of data science, artificial intelligence, and machine learning to process vast amounts of data from various**

sources. Invest in advanced data analytics to derive actionable insights that enhance decision-making in times of uncertainty.

4. **Embed Ethical Considerations: Prioritize ethical dimensions in decision-making processes, especially when employing automation and AI in warfare. Carefully consider issues of accountability, transparency, and potential unintended consequences to ensure responsible and appropriate use of technology.**
5. **Disseminate via Global Collaboration and Partnerships: Recognize that digital warfare is a global challenge, and foster collaboration and partnerships between different defence organizations, allied nations, and private sector experts. Emphasise action-focused collaboration to address real challenges and build trust among partners.**

By adopting these five principles, both individuals and organizations can navigate the complexities of digital transformation and AI in the defence sector. Embracing cross-disciplinary collaboration, agility, data-driven decision-making, ethics, and global partnerships will help ensure that defence organisations are well-prepared to meet the challenges of the future and maintain the safety and security of their nations.

CALL TO ACTION

Following the success of this inaugural international conference, DDRC will shortly be announcing further collaborations and events for the 2023/24 academic year. We will be in touch with details in due course.

DDRC would be very interested to hear from Defence experts, academics and industry practitioners with skills/experience relevant to the Defence sector, and to the challenges laid out in this paper. If you are interested in participating, please contact **Professor Alan Brown**.

Further publications and white papers on the subject of Defence AI, data science and technology improvements can be found **on our website**.

For more information, please contact: info@ddrc.uk

www.DDRC.UK

DDRC
DEFENCE DATA RESEARCH CENTRE