techUK
FOR WHAT COMES NEXT

DefTech: Technology Transforming Defence

November 2024

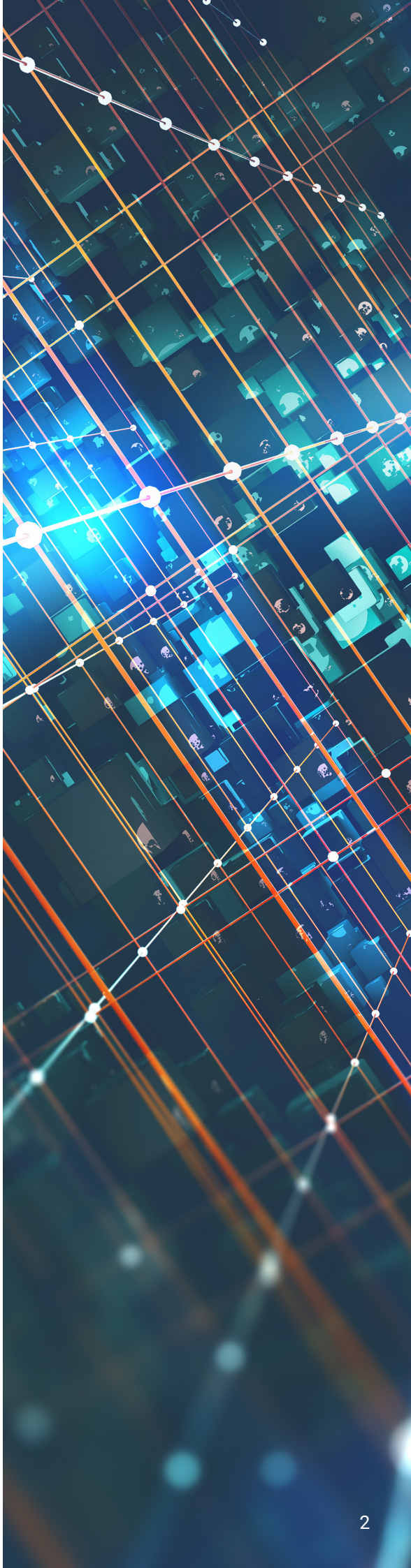
Defence Technology (DefTech) will not only revolutionise the way military operations are conducted but, in the process, transform the Defence industry itself, opening the market up to new technologies and new suppliers including start-ups and SMEs, and those with dual-use capabilities.

Advances in sensing allow ever greater exploitation of the electromagnetic spectrum, enhancing intelligence, surveillance and recognisance (ISR) capabilities. Situational awareness, target acquisition, and threat detection depend on this, as does secure communication between platforms and war fighters.

Autonomy will shape the deployment and positioning of sensors on uncrewed systems in the air, surface or sub-surface, as well as the delivery of weapons systems and logistics.

However, the value of DefTech depends on its ability to draw data from all five domains together, processing and analysing, turning it into something actionable by the end-user. The use of Artificial Intelligence (AI) and Large Language Models (LLMs) will affect everything from Command and Control (C2) across land, sea, air and space, to anticipating vehicle maintenance requirements and managing stocks of spare parts.[1]

The development of platforms and systems across all domains and scales – from Tempest to Tactical Communications – designed to utilise these capabilities creates a new urgency in understanding what this means for Defence. A radical transformation of the entire Defence enterprise is required, spanning the Defence centre, delivery organisations, end users, the DefTech community and wider society.



Context

The conflict in Ukraine has provided the most graphic and costly vision of how future wars are likely to be fought, demonstrating that victory will be determined not solely by conventional mass, but also the ability to develop, integrate and deploy advanced technologies at speed. The war in Yemen has further highlighted the ability of non-state actors to pose a serious, conventional threat using comparatively inexpensive commercial off-the-shelf (COTS) capabilities.

The last decade has been dominated by platforms and hardware including those described by the House of Commons Defence Select Committee as 'over-complex, over-budget, over time'.[2] Despite the visions of those in leadership, when it comes to emerging technologies, the reality means procurement processes inhibit their acquisition, and legacy systems across the Defence Enterprise prevent their exploitation.

If the UK could be – as in the assessment Chief of the General Staff General Sir Roly Walker – three years from war[3], the battle of procurement is surely already being waged. Or at least it is by potential adversaries. Any presumptions about procuring at pace in times of crisis, should be countered with the experience of meeting the demand for Personal Protective Equipment during the COVID-19 pandemic.[4]

The UK requires:

- A Ministry of Defence (MOD) that can empower the sector to innovate through clear problem setting, with the resources to rapidly procure its products cost effectively, and then pull them through to the end-user in the shortest possible time.
- A strong, dynamic DefTech sector to ensure that the UK remains at the forefront of innovation, providing solutions to those problems articulated and encountered by MOD, and learning the lessons from how other industries have achieved transformation.
- A wider civil society that acknowledges the existential threats facing the West, and the need for both government and private investors to not just remove existing barriers but encourage and enable greater investment.

What is DefTech and what are techUK members doing in this space?

DefTech can be defined as any app, software, or technology that allows a constituent of the Defence enterprise to digitally access, manage, gain insight into and/or efficiently and securely prosecute military operations, the maintenance of capability and/or the acquisition and deployment of new capability.

The application of AI within the warfighting domain dominates public understanding of what emerging technologies and particularly the role (or lack of) that humans will play in that.

The reality is there are myriad ways in which emerging – and indeed emerged – capabilities will impact Defence, tackling challenges which are by no means unique to the Defence enterprise. This includes everything from predicting vehicle spare part requirements, multi-year contract processing, through to management of the Defence estate.

techUK members are at the forefront of this technological revolution:

2iC

2iC is a global leader in digital interoperability in the battlespace with proven off the shelf software that connects and controls systems and devices not originally designed to work together.

Using open standards, 2iC software enables the rapid digital integration and coordination of diverse systems and devices which are typically uncrewed, wearable, or vehicle borne. 2iC software uses any available communication bearers and is designed for use in the modern battlespace.

2iC's distributed resilient platform is an underpinning technology that enables iterative adoption of DefTech.

2iC is a sovereign UK Small Enterprise (SME) with customers that include the UK Ministry of Defence, the United States Department of Defense, the Australian Department of Defence and the New Zealand Defence Force along with globally recognised Systems Integrators and Equipment Manufacturers. 2iC has significantly contributed to the development of digital interoperability standards in Defence and Healthcare.

GemaSecure – Unmanned Autonomous Systems

GemaSecure Ltd is an established, UK Sovereign, specialist SME developer of ultra-fast, ultra-secure, ultra-low power, high performance, voice, video, and data technologies (FPGA based hardware and embedded secure software applications) focused on the processing of huge amounts of data incredibly quickly with its range of hardware devices able to interrogate, analyse, and process between 1GbE and 400GbE of data throughput in <20µS using only 10 Watts of power (up to 4Gb data throughput) – max 350 Watts (400Gb data throughput).

Its modular, multi-functional approach enables it to adopt a more creative, problem-solving approach that provides a compelling answer to the customer's problems in a manner that they might not have previously considered or even thought was possible.

GemaSecure thrives on simply being presented with the challenge of delivering against the required outcome... but not being told how that outcome should

be achieved. This approach enables the company to adopt latest technologies in an agile and cost-effective manner that may not have been imagined by those commissioning the original end-user requirement.

Arondite - Embracing Data

Arondite is a UK-based defence deep tech company building the foundational software and AI to enable the scaled use of sensors, robots, and autonomous systems.

As the number of autonomous systems grows and Defence becomes more software-defined, battles are lost when systems can't collaborate. Arondite solves this problem by building the smart connective tissue needed to enable human-machine teaming, reducing cognitive burden on the war fighter and delivering decisive operational results.

Its flagship software platform, Cobalt, enables users to manage their battlespace together with their autonomous systems, rapidly connecting data sources and physical assets. Dynamic management of mission data and AI models automates the creation of insights and intelligence, presenting all the information required to make decisions in a secure and flexible user interface. Cobalt's extensible architecture ensures interoperability by design, so war fighters can exploit existing assets and swap in new systems as operational needs require.

Challenges

The challenges facing Defence in finding and procuring innovative new technologies have been expressed sufficiently already and the challenge of inflexible, outdated acquisition processes well-rehearsed.

The problem is that the oft-repeated ‘solutions’ offer little by way of practical guidance. The need for agile procurement, a software-first or best-practice approach all regularly feature in discussions. For the MOD - Strategic Command, Defence Equipment & Support (DE&S), Defence Digital, and the Defence Science Technology Laboratory (Dstl) – plus at least four innovation units per Frontline Command, such phrases are rendered meaningless.

The following section aims to offer workable suggestions for how the MOD and DefTech industry can both work more effectively to ensure that the right technology finds the end-user at a fair price, learning the lessons from how other countries and industries have managed this revolution.

Ministry of Defence

Recommendation 1: Forget GDP, think capabilities

The political debate around Defence is too heavily dominated by discussions about percentages of GDP committed to spending. This has become a political tool implying that the higher the number, the more seriously Defence is taken. In practice, such a figure is of little real value as economies fluctuate, and higher spending does not necessarily equal greater capability or mass.

The MOD should express explicitly what the UK regards as core sovereign capabilities and those where it should look to develop with partners such as NATO, the Joint Expeditionary Force[5] or AUKUS. This would send industry a clear demand signal, from which then flows budgetary decision-making.

Recommendation 2: Who, what, where?

The MOD must urgently look to rationalise the bewildering number of innovation and delivery units stretching across the Defence ecosystem, each with their own ways of operating and contracting (before even considering procurement frameworks). This inevitably leads to inefficiencies with techUK members (and MOD employees) sharing cases where different units are pursuing similar technologies and services needlessly.

The MOD should look at the model of the Defense Innovation Unit within the US Department of Defense tasked explicitly with 'accelerating the adoption of leading commercial technology throughout the military and growing the national security innovation base'. Such a body would require acknowledged authority over Front Line Command (FLC) innovation units to ensure they do not pursue separate technologies based on identical technology stacks, and that where success occurs it is pulled through into other services.

Such an organisation would be rendered impotent from the start though without having a similar window into Dstl. Dstl must do more to ensure that it is not developing capabilities that are already commercially available. Again, techUK members report with frustrating experiences of discovering that Dstl is a step behind industry, for instance in pursuing UAS systems, to address problems they have already solved.

Recommendation 3: Bring problems not solutions

Rather than articulating requirements upfront, the MOD should expand the use of problem statements for acquiring capabilities, shaped with input from the end-user. When circulated through a network of industry bodies and trade associations, such an approach will reach the widest range of providers with potential answers.

This is easy to do when the problems and capabilities are new. The real challenge comes when replacing existing or legacy technologies, where the requirement and expectation can be subconsciously pre-defined by past experiences such as in the tactical communications space.

His Majesty's Government Communications Centre (HMGCC) has adopted such an approach. Focusing on defining the problem rather than the requirements, means they *'can think freely and work in an agile and iterative way'*.[6] Speaking at techUK recently, CEO George Williamson, shared the problem of batteries operating in extreme temperatures, with the solution coming from a company specialising in frozen food distribution.

Finally, if the problem can't be defined in a few paragraphs, it hasn't been defined well enough. A recent call by the US DoD Defense Innovation Unit looking for an *Enterprise Workflow and Reporting Platform* identified the problem, outlined the use requirements, desired solution attributes, and potential obstacles, all in under 700 words.

Do not assume anything.

Recommendation 4: What got us here…

Not assuming the solution, also means not assuming its source. The MOD should look to empower commercial teams to consider the widest possible group of suppliers when seeking capabilities, with the contracting resources to match. This means removing unnecessary requirements placed on SMEs - such as declarations on asbestos management for IT consultancy work as reported by a member – and disproportionate levels of liability insurance. It also means finding ways to accommodate new supplier groupings such as 'defence shoals' where a group of SMEs bid as one entity and share the administrative responsibilities between them.

Such an approach will require a new approach to risk. The MOD should publish guidelines giving complete transparency as to how it calculates risk, giving companies insight on what they need to do it mitigate it.

Recommendation 5: Mind the Gap – the innovator and the end-user

Part of defining a problem, is knowing there is a problem is in the first place. FLCs already employ Chief Technology Officers with previous commercial experience. The MOD should now look to recruit reservists from industry with a practical understanding of technological applications, who can be deployed at a tactical rather than purely strategic level. A critical component in problem-statement drafting, they would be tasked with identifying gaps and flaws in current processes where technologies could provide solutions. They would have a mindset that sometimes a quick fix to an individual problem tomorrow, is better than the promise of an integrated solution in five years' time.

Such deployments could include Operation Cabrit, the British Army's commitment to the enhanced Forward Presence (eFP) in Estonia, or the Carrier Strike Group 2025.

Recommendation 6: All about the Data

Success on the battlefield will increasingly depend on the ability to turn raw data into practical intelligence. Therefore, the MOD needs to understand what data it is contracting to receive from its platforms. This means standardising the process by which it facilitates the exchange of datasets, working between manufacturer, service provider, and the end-user.

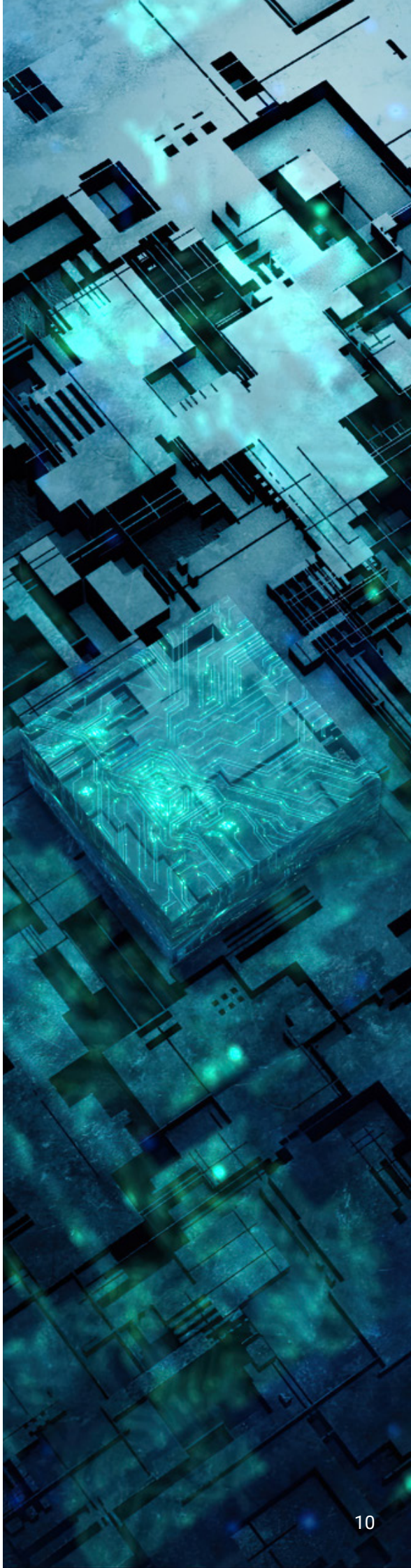
The systems that will do this though require training. The Ministry of Defence's Defence AI Centre should look at how it can work with industry partners to provide the DefTech sector with workable, synthetic datasets across all domains in a single repository that allow companies to start preparing products for the market. The US Space Systems Command's Unified Data Library currently draws together and distributes datasets from dozens of commercial, academic, and frontline sources for use by partners across the Defence enterprise.[7]

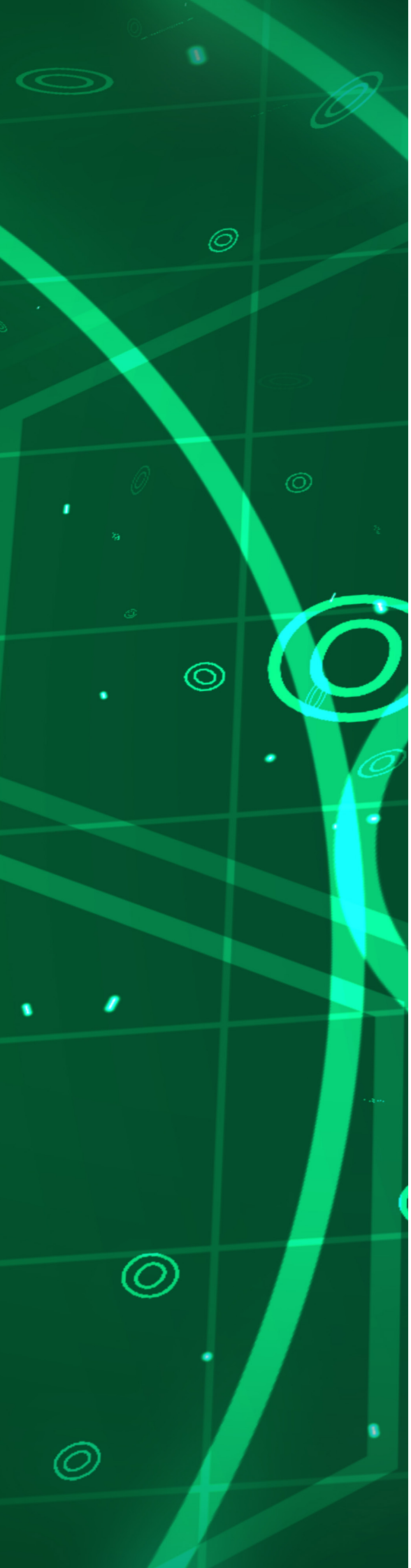
There is precedent for this beyond Defence as well. The Financial Conduct Authority's Digital Sandbox provides the FinTech sector access to GDPR compliant dataset to 'help enable experimentation and scaling for proof of concepts'.[8]

Industry

If the MOD needs to communicate in problems, industry should talk solutions. A challenge for industry, and particularly for those in research and development, is presenting a product in terms of what its deployment means for the end-user in practice. When pitching and presenting, do not assume anything is obvious to the audience. Think battlespace and not laboratory.

And if it works, tell others. When talking about procurement problems, it would also be unfair not to highlight those parts of the MOD which are pushing for new ways of operating, such as Commercial X, and the Future Capabilities Innovation within DE&S. Industry should therefore play its part in 'joining the dots' between the different parts of the MOD when things work well or otherwise.





As highlighted by Alex Cresswell, outgoing CEO of Thales UK, there is a paradox in the UK (although found elsewhere in Europe as well) where respect for the Armed Forces is not matched by attitudes towards the companies arming and protecting those troops in conflict. Inappropriately applied Environmental, Social and (Corporate) Governance criteria and reports of de-banking of Defence companies[9], particularly amongst SMEs, means the sector still struggles to attract much needed support from financial institutions, investors, and pension funds.

As the West comes to terms with an increasingly unstable geopolitical landscape, it is more important than ever for British society to recognise the value DefTech companies play in upholding and supporting the rules-based international order. In the words of Cresswell, 'we should be preparing ourselves much more for the threat that is posed to our society. History shows that by preparing, we're less likely to be in a conflict'.[10]

Many thanks to the techUK members and those within the Ministry of Defence who shared their experiences and ideas that fed into this paper.

References

1. https://assets.publishing.service.gov.uk/media/65bb75fa21f73f0014e0ba51/Defence_AI_Playbook.pdf
2. https://www.gov.uk/government/speeches/defence-procurement-minister-oral-statement-on-the-integrated-procurement-model-28-february-2024
3. https://www.rusi.org/research-event-recordings/keynote-recording-sir-roly-walker-chief-general-staff
4. https://mcusercontent.com/cd87957c772f7bc847e157914/files/8efe095d-9a5b-3fee-0d1d-54a53dd2ed05/Behind_the_Masks_Summary_EMBARGOED.pdf
5. https://www.rusi.org/explore-our-research/publications/commentary/joint-expeditionary-force-digital-better-way-deliver-defence-tech
6. https://www.hmgcc.gov.uk/co-creation/
7. https://www.ssc.spaceforce.mil/Portals/3/SSC's%20Unified%20Data%20Library%20participates%20in%20Army's%20Project%20Convergence%202_1.pdf
8. https://www.fca.org.uk/firms/innovation/digital-sandbox
9. https://www.thebanker.com/ESG-concerns-lead-European-banks-to-debank-defence-firms-says-EU-defence-body-1719481540
10. https://www.theguardian.com/business/2024/mar/26/im-not-profiting-from-misery-im-averting-more-thaless-uk-boss-on-making-missiles-for-ukraine

Further information

techUK's Defence Programme works to help the UK's defence technology sector align itself with the Ministry of Defence - including Defence Digital, DE&S, innovation units and Front Line Commands - through a broad range of activities including private briefings and early market engagement events.

For more information, please contact:

Jeremy Wimble, Programme Manager, Defence, techUK
E jeremy.wimble@techuk.org

techUK
FOR WHAT COMES NEXT


linkedin.com/company/techuk


@techUK


youtube.com/user/techUKViews


info@techuk.org

Image credits | iStock by Getty Images