University of Exeter

Exeter Defence, Security and Resilience

Defence, Security & Resilience Compendium

February 2025

Contents

Foreword

Professor Lisa Roberts, President and Vice-Chancellor

Welcome to this special collection of articles on issues relating to defence, security and resilience, which I hope will be a useful compendium for busy decision-makers and their offices. I also hope it will appeal to anyone with an interest in the defence, security and resilience sectors.

The articles provide some fresh perspectives in this uncertain and contested environment. The modern challenges we are facing require greater partnership between Government, business, and academia, and the University of Exeter is proud to play its part in seeking solutions alongside our valued partners.

To enhance the University's growing reputation in this field, we have recently established the *Exeter Defence, Security and Resilience Network*. This brings together more than 220 interdisciplinary academics from across the University.

The network promotes strong and agile internal and external collaboration with our strategic partners, research councils and government, and has an extensive breadth of work. This ranges from leadership and strategic decision-making to vital geopolitical understanding and policy support; virtual reality to smart cities; and quantum computing to incel motivation.

Our University is also home to world-renowned climate change and sustainability scientists, whose work is influencing approaches in defence, security and resilience. University academics are at the forefront of cyber security and technology advantage, as well as the consideration of AI in war. Our interdisciplinary approach promotes the convergence of science with the legal and ethical considerations.

We hold an extensive range of partnerships with UK and global universities and other organisations, and we can bring global perspectives and additional expertise to our research, consultancy and education provision.

Through the Defence Data Research Centre (DDRC), a partnership between Exeter and the Universities of Liverpool and Surrey, our Digital Catapult and the Defence AI Centre brings a multi-disciplinary approach to improve the use of data in the defence community. Our University is also playing an increasing role in the growing AUKUS space, with the innovative Global Executive MBA in Defence and Space delivered in partnership with universities in Australia and the United States.

This compendium offers many highlights. It contributes to the ongoing Strategic Defence Review, raises the profile of topics often overshadowed but in need of urgent policy attention, and prompts consideration of wider defence and security issues.

First is an article by **Dr David Blagden,** who has worked with the Royal Navy, the Ministry of Defence's (MoD) Futures Centre, and served as a Specialist Adviser to the House of Lords' International Relations and Defence Committee. In **'Augmenting UK Nuclear Posture: Considerations and Options'** his research considers three layers of possible augmentation, from the relatively modest but immediate and necessary, through to the more ambitious and speculative. Given the centrality of the nuclear deterrent to UK defence, this article provides some clear pathways for consideration.

Professor of Practice in Strategy and Security, Frances Tammer, brings her decades of MOD and Cabinet Office experience to bear. In her article on the **imminent Iranian nuclear threshold situation,** she raises the frightening question of whether it could now be too late to respond, as the focus has been elsewhere.

The prospect of an Iran with nuclear weapons must be faced.

With his long experience of working with multinational companies and Government departments, **Professor Alan Brown brings a practical and commonsense approach as to how we deliver AI at scale.** In an increasingly constrained financial environment in which there is a pressing need for strategic advantage, he provides a holistic and pragmatic approach. His latest book is entitled '*Surviving and Thriving in the Age of AI: A Handbook for Digital Leaders.*'

Professor Voicu Ion Sucala, Head of the Engineering Department, is Vice-Chair of the Research, Innovation and Knowledge Transfer Committee at the Engineering Professors' Council, and a Senior Fellow of The Higher Education Academy. His research focuses on modelling, simulation, digital twinning and optimisation of manufacturing processes, technology innovation and entrepreneurship, industrial organisation management, and engineering education. In this article, he writes about the **shortfalls in educational provision in disruptive and novel technologies, but highlights where the University of Exeter is making a key difference.**

Straddling the operational and policy dimensions are the articles by **Professor Aurel Sari on unpicking the law of armed conflict (LOAC); Professor Fiona Charnley and collaborators on how a circular economy could be achieved;** and **Dr Jesse Abrams on how climate change will impact military operations.**

Professor Aurel Sari is one of the principal experts on the legal aspects of hybrid warfare. He works with NATO, and is a Fellow at the Supreme Allied Powers Europe (SHAPE). He argues that a gap is appearing between the Laws of Armed Conflict and public perception, citing the recent conflict in Gaza as an example. Professor Sari also collaborates with Australia and the US on the development of space law.

Compiled with assistance from the Defence Science and Technology Laboratory (Dstl) as part of the UKRI NICER Programme's CEctor project, the article T**owards a Circular Economy within the defence and security Sectors,** led by **Professor Fiona Charnley,** indicates how a circular economy presents a solution to the systemic challenges faced by MOD organisations.

Defence accounts for 50% of the UK central government's greenhouse gas emissions, and the report outlines the issues facing the sector, from the escalating threat of climate change to decarbonisation targets, supply chain volatility, energy geopolitics, material availability and outdated systems and infrastructure.

Professor Fiona Charnley is Professor of Circular Innovation and Co-Director of the Exeter Centre for Circular Economy.

Part of the University of Exeter's Global Systems Institute, **Dr Jesse Abrams's** interdisciplinary research focuses on understanding and quantifying human-induced environmental change, with a particular emphasis on climate change and biodiversity loss. His article asserts that, whilst the MoD understands the need to reduce its carbon footprint and has begun initiatives to transition to cleaner energy sources and more efficient technologies, there needs to be an acceleration in adapting military infrastructure, equipment, supply chains and operations accordingly.

The workforce remains the most important resource within defence. The work by **Professor Esther Reed on the 'Ethics of Moral Injury'** highlights the issue of inadequately explicit attention to moral health at policy levels, and research into its implications for retention and recruitment. It raises issues about how the Armed Forces handle inappropriate behaviours. Professor Reed, widely acknowledged as an expert in military ethics, addresses this issue through the lens of theological ethics and moral philosophy.

The compendium is rounded off with **Dr Lewys Brace's research on the changing nature of domestic online extremism and self-radicalisation.** Specialising in data science, extremism, terrorism, cybercrime, and Open-Source Intelligence (OSINT), he is the Co-Director of the University's Centre for Computational Social Science (C2S2). Focusing

on the growing phenomenon of self-initiated terrorists, his research shows that these cases have been notoriously hard to detect due to their nature, and the fact that technological affordances are driving an increase in younger individuals forming their own bespoke ideology that aligns with their own personal experiences.

I hope you find the articles contained within this compendium to be useful and informative, and that they provoke thoughts, discussions, and new ways of thinking. As we look to address the challenges of the 21st century, it is our great hope that the research and expertise of the University of Exeter can play a key role in developing solutions and fostering a more secure world.

General (Retd) Sir Patrick Sanders KCB CBE DSO

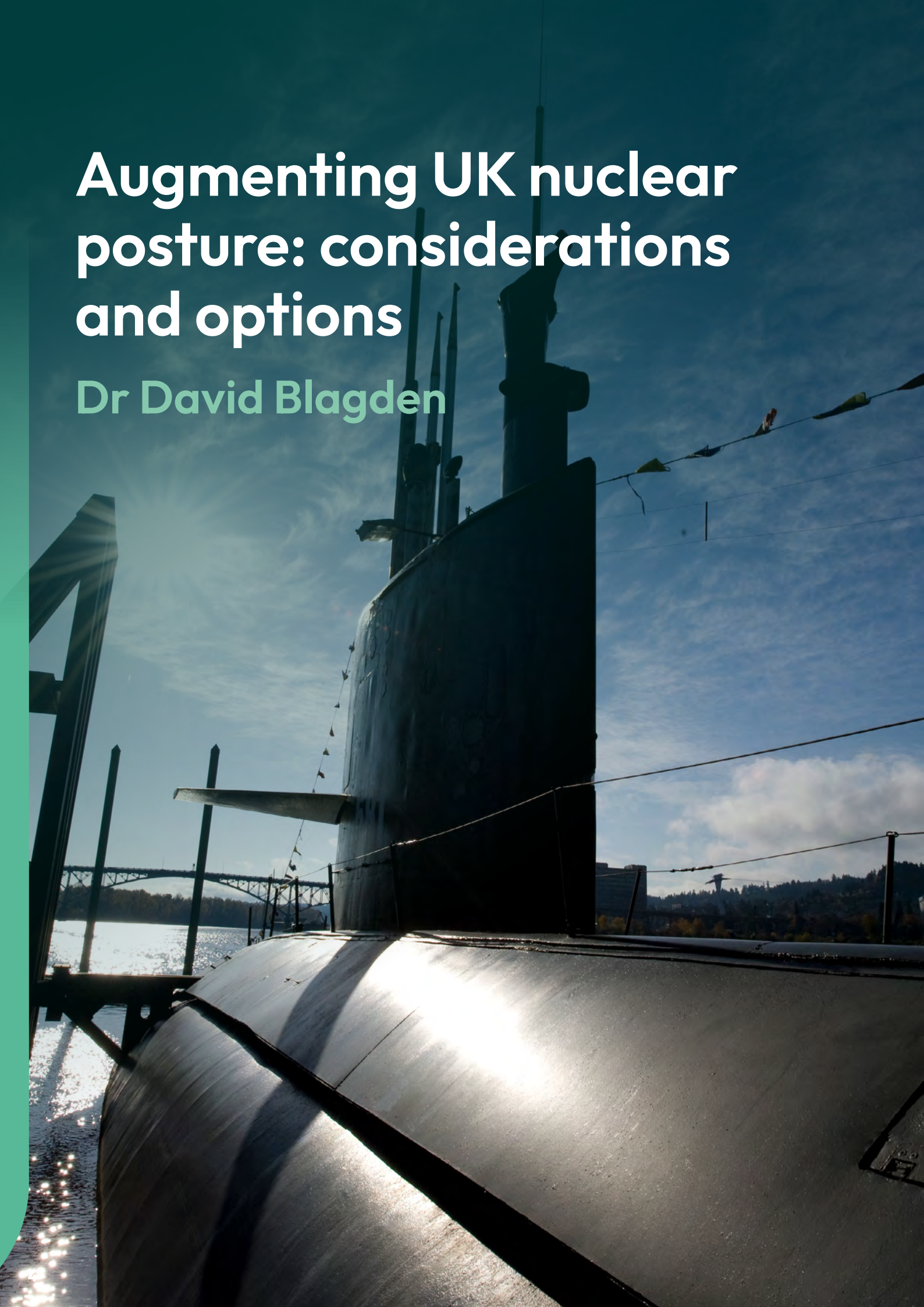
I really welcome the timely publication of this anthology. As one of the UK Armed Forces six Chiefs of Staff over the last five years in two separate roles, most recently as Chief of the General Staff (CGS), I placed a huge premium on the contribution made by academia in providing independent analysis on the range of issues exercising policy makers, intelligence, agencies, and military planners. This independence, enriched and underpinned by academic rigour, offers alternative and fresh perspectives, has the benefit of distance from political expediency, and can serve as a vital antidote to the groupthink to which all government and military institutions can be prone.

I can think of few better qualified or equipped to compile this collection than the University of Exeter whose reputation and impact in the sphere of strategic studies, international security, defence, and climate change is formidably strong and only increasing.

And it is timely. The Strategic Defence Review is wrestling with many of the themes contained herein. And in the face of intense fiscal pressure seeks to craft a national security strategy and a defence posture that must reconcile: global interests and ambition; NATO commitments, war in Europe and the Middle East; the unwelcome reminder that war is seldom short and involves attrition (so stockpiles, mass and industrial depth really matter); and the imperative to secure the competitive edge provided by technology (and in particular an impending Cambrian explosion of autonomous systems). No small task. I know, having been involved in the last three defence reviews, that often the greatest wisdom comes from without. This anthology should make a significant contribution to that end.

Augmenting UK nuclear posture: considerations and options

Dr David Blagden



Russia continues to increase its bellicosity towards NATO. Yet, with China having ascended to become a true US peer-competitor in the western Pacific, Washington faces a clear strategic imperative to focus its military efforts in Asia rather than Europe.

European NATO members will highly likely be required to do more to secure their own region, with less reliance on US power to safeguard all member states simultaneously. And Russia's stumbling conventional military operations in Ukraine belie a wealth of tactical nuclear weapons; such a combination may push Moscow to resort to its atomic toolkit if it enters or anticipates a wider conflict with NATO yet also assesses that NATO states would have few credible response options.

Taken together, such circumstances necessitate reconsideration of existing UK nuclear posture's adequacy. Three possible augmentations merit consideration, from the relatively modest (but immediate and necessary) through to the more ambitious and speculative:

1. Increasing current capacity, to preserve existing credibility;
2. (Re)adopting a sub-strategic posture, to dissuade adversaries from counterforce nuclear strikes; and/or
3. Adding to the arsenal of UK nuclear weapons and/or delivery systems, possibly via a new tactical option, to diversify the UK's nuclear deterrent.

Running to stay still: increase capacity to sustain Continuous At-Sea Deterrence in an overstretched Navy

Merely sustaining the existing Continuous At-Sea Deterrence (CASD) posture is placing tremendous strain on the Royal Navy.

Records for ballistic missile submarine (SSBN) deployment lengths have reportedly been broken twice in the past year, with patrols of 195 and then 201 days.[1] Such reports suggest a force that is having to stretch its few available hulls and people further and further to sustain commitments. These exertions hurt retention, recruitment, maintenance and training. Other open-source reporting suggests that the availability of the attack submarine (SSN) fleet necessary to protect the SSBNs – as well as fulfilling multiple other missions – is also currently at alarmingly low levels,[2] the Royal Air Force's fleet of just nine P-8 maritime patrol aircraft (MPA) is too small to sustain continuous wide-area coverage.

As such, UK nuclear forces need 'augmenting' just to preserve existing credibility. Resources are needed to recruit, train and retain the people necessary to keep the *Vanguard*-class SSBNs and their weapons at sea, to maintain the hulls and their weapons,[3] to ensure there are no further delays in bringing the *Dreadnought*-class successor SSBNs into service (already a decade later than planned),[4] and to ensure

1 James Knuckey, 'HMS Vengeance: Vanguard-class submarine's secret monster deployment beneath the waves', Forces.net, 21 March 2024, www.forces.net/services/navy/hms-vengeance-vanguard-class-submarines-secret-monster-deployment-beneath-waves (accessed 01/07/2024).

2 One open-source intelligence compiler suggested that – as of 29/06/2024 – only one RN SSN (the last remaining Trafalgar-class boat) was available for operations: Ryan Ramsey, X.com posting, 30 June 2024, x.com/ssn14co/status/1807130533446754597?s=46 (accessed 01/07/2024).

3 Old hulls potentially increase a number of risks, both to safety (of the crew and their deadly payloads) and to operational effectiveness (e.g. if ageing boats acquire noise shorts that enable hostile counter-detection).

4 The UK's originally stated policy on the Vanguard-class submarines' replacement saw them leaving service from 2022, with a successor SSBN class taking over on the same schedule: HM Government, The Future of the United Kingdom's Nuclear Deterrent (Norwich: HM Stationery Office, December 2006 (Cm 6994)), https://assets.publishing.service.gov.uk/media/5a7c3ec8ed915d76e2ebc0dd/6994.pdf (accessed 01/07/2024), p. 10. The current (as of 2021) official position is that the first of the Dreadnought-class SSBNs will actually now enter service in the early 2030s: UK Ministry of Defence, 'Dreadnought submarine programme', Gov.uk, 16 March 2021, www.gov.uk/government/collections/dreadnought-submarine-programme-the-facts (accessed 01/07/2024).

protection of SSBNs against adversaries' advancing anti-submarine capabilities (necessitating more SSNs, frigates, MPAs, anti-submarine helicopters, remotely-operated surveillance systems, and so forth). As hostile powers expand their offensive capabilities, the UK's nuclear forces must keep running just to stay still.

Enhanced resolve within the existing system: a new declaratory posture?

The existing nuclear force consists of four SSBNs, each carrying a number of Trident D5 missiles armed with some amount of UK warheads. Together, these weapons and hulls sustain CASD patrols. It would be possible to augment the UK's nuclear forces within these existing parameters. Such augmentations could include reverting to an explicit doctrinal statement of Trident's 'sub-strategic' potential, which was the UK position in the 1990s,[5] but subsequently, slipped out of official usage, even as the UK Holbrook warhead's technical capacity to be used with greater accuracy and in different yield-states has reportedly increased.[6] This could help to dissuade adversaries from counterforce nuclear strikes on UK/NATO targets, especially in hypothetical conditions in which an adversary believes that an Asia-focused US is distracted or uninterested while the UK and France are unlikely to escalate to a world-ending countervalue exchange. However, sub-strategic use would bring real risks too, notably of an adversary inferring that a 'sub-strategic' Trident launch was actually the opening salvo of an all-out NATO nuclear strike (and retaliating accordingly).

Such augmentations could also include enhancement of UK nuclear command and control (C2) via some variant of TACAMO ("take charge and move out") capability. Throughout the UK's SSBN-based nuclear era, this function has been delivered by a 'Letter of Last Resort', providing the Prime Minister's instructions to the deployed submarine's command team on how to proceed if they assess that the UK's strategic leadership has suffered a decapitation strike (and thereby hopefully removing adversaries' incentive to attempt such a strike in the first place). However, the 'Letter of Last Resort' system has historically relied on there being only a single plausible culprit for such a strike, namely the USSR/Russia. While Russia is still by far the most likely *and* most capable potential nuclear aggressor against the UK, there are now more (a) hostile nuclear powers and (b) escalation scenarios to consider, meaning that a posthumous "Fire at the Kremlin!" order may be inadequate.

Adding to the arsenal: diversifying the UK's nuclear weaponry

Third, and most contentiously, new nuclear weapons and/or delivery systems might be added to the UK arsenal, for two possible reasons. For one, it may be worth using a latent tactical weapons programme[7] to hedge against lessened US commitment. Such US reticence could leave NATO with an escalatory gap that a risk-acceptant adversary may feel it could exploit for battlefield gain. Obviously, crossing the threshold back to a fully functioning nuclear 'dyad' of air-launched and submarine-launched weapons would come with steep political and financial costs.

5 House of Commons' Defence Select Committee, The Future of the UK's Strategic Nuclear Deterrent: The Strategic Context (Eighth Report of Session 2005-6) (London: Parliament, 30 June 2006), publications.parliament.uk/pa/cm200506/cmselect/cmdfence/986/986.pdf (accessed 01/07/2024), pp. 12-13.

6 E.g. Hans Kristensen, 'British submarines to receive upgraded US nuclear warhead', Federation of American Scientists, 1 April 2011, fas.org/publication/britishw76-1 (accessed 01/07/2024). Note that the title of this article is a misleading simplification; it discusses UK adoption of the higher-utility Mk4A re-entry body, not wholesale UK usage of a US-made warhead. More recently, UK Ministry of Defence officials have explained that the next-generation UK warhead will again be "not exactly the same" but with "a very close connection" to its US equivalent, implying that such 'sub-strategic' potential will remain: House of Commons' Defence Select Committee, 'Oral Evidence: MOD Annual Report and Accounts 2019-20' (HC1051) (London: Parliament, 8 December 2020), committees.parliament.uk/oralevidence/1350/pdf (accessed 01/07/2024), Q31.

7 The smallest version of the UK's last tactical nuclear weapon – the WE.177A, which was retired in the 1990s – reportedly weighed ~272kg (with reported 0.5kt or 10kt yield options). Meanwhile, the (conventional) warheads of the UK's current Storm Shadow air-launched cruise missile (ALCM) and US-sourced Tomahawk submarine-launched cruise missile (SLCM) both reportedly weigh 450kg. As such, it should be feasible to swiftly generate rudimentary UK air- and/or submarine-launched tactical nuclear options – or at least generate the contingency plans to do so – if HM Government resolved to make the resources available.

However, if US commitment falters, or Moscow perceives it to do so, there would again be a grave risk of an aggressor judging that they can get away with waging massive conventional and/or tactical nuclear war without the UK or France resorting to an apocalyptic countervalue exchange.

This is especially true if London and/or Paris are reluctant to use their submarine-launched ballistic missiles as 'sub-strategic' weapons, given such an approach's downsides (see above). If a UK tactical nuclear capability is near or fully realised, this risk may be minimised, albeit with obvious drawbacks.

In addition, as technological progress renders the oceans less 'opaque',[8] it is time to start thinking about how the UK's wholly SSBN-based nuclear force can be hardened and/or diversified to ensure its resilience as submarine-hunting advances. Many potential innovations in SSBN detection can and will be countered by technological or doctrinal adaptations. But if technological progress *does* start to meaningfully degrade oceanic opacity, thereby reducing SSBNs' ability to survive, augmenting UK nuclear posture with some other delivery system or systems may become necessary. It would be prudent to begin contemplating responses to that possibility well in advance of it arriving.

8 See e.g. Elizabeth Mendenhall, 'Fluid Foundations: Ocean Transparency, Submarine Opacity, and Strategic Nuclear Stability', Journal of Military and Strategic Studies 19:1 (2018), pp. 119-158.

What happens if Iran becomes a nuclear state?

Professor Frances Tammer

On 19th July 2024, the then US Secretary of State Antony Blinken relayed the stark assessment that Iran's breakout time, the amount of time needed to produce sufficient weapons grade material for a nuclear weapon," was now probably one or two weeks"[9]. This assessment, almost certainly based on all-source fused intelligence, and agreed across the US Intelligence Community, represents the shortest breakout time[10] the US has publicly declared.

The UK Joint Intelligence Organisation, which provides the cross-government all-source intelligence assessments, is highly likely to have a similar assessment, as it will have received the same intelligence feeds as the US Intelligence Community. As part of its influencing strategy and to ensure there is a common intelligence picture, Israel almost certainly will have disseminated some raw intelligence and its own intelligence assessments to its trusted Western partners plus the same or sanitised intelligence assessments to selected regional countries and the International Atomic Energy Agency (IAEA)[11,12].

Iran has always maintained its nuclear programme is entirely peaceful and not for weaponisation, but the evidence clearly points to the opposite. In addition, Iran creates deliberate ambiguity for the International Community through carefully planted ambivalent statements about its intent. It has frequently threated to withdraw from the Nuclear Proliferation Treaty.

Does this mean that Iran already has a testable nuclear device? Not entirely, but it is fast approaching that moment. There are many elements to producing a nuclear device. Under the terms of the 2015 Joint Comprehensive Programme of Action (JCPoA) 10-year duration, Iran agreed to dismantle much of its nuclear programme and open its facilities to more extensive inspections by the IAEA in return for billions of dollars of sanctions relief.[13]

9 CNN,19 July 2024.

10 This is the amount of time it could take Iran to produce enough fissile material for nuclear weapons.

11 The continuous nature of this Israeli influencing strategy was witnessed in June 2024 at a joint US/Israeli conference in Washington when Israeli intelligence agencies produced new information about computer modeling by Iranian scientists that could be used for research and development of nuclear weapons.

12 U.S. and Israel agree to reconvene Iran meeting cancelled after Netanyahu accusations (axios.com), 25 June 2024.

13 Main Text (state.gov) Signed by China, the EU Commission, France, Germany, Russia, UK and US.

In simple terms, there needs to be the following:

Key Requirement	Current Iranian Position	Comments
Fissile Material **Sufficient stockpile quantities and purity**	Has roughly 142 kilograms of 60% purity of enriched uranium, an increase of more than 20 kilograms since Feb 2024.[i] This is significantly above the 3.67% permitted under the 2015 Joint Comprehensive Programme of Action (JCPoA[ii]) when Iran agreed to reduce its stockpile of low-enriched uranium by 98% to 300kg, for a period of 15 years.	Iran would need roughly 42 kilograms of 90% enriched uranium for one nuclear bomb. Hence it has sufficient for the production of three bombs. US and Israeli intelligence assessments maintain it will take several weeks to enrich this amount of uranium to 90%, the level needed for a nuclear weapon.[iii] In early 2023 the IAEA found traces of uranium enriched to almost 84% purity, although Iran said it was a mistake.[iv] There is no credible civil energy use for uranium enriched above 60%.
Centrifuges **Machinery for enrichment**	Progressively installed higher-powered centrifuges to achieve the above; numbers have not been cut.[v]	Under the JCPoA, Iran's centrifuges would only enrich to 3.67%, and the operational number would be reduced by two thirds.
Delivery Method	For example, in October 2023, Iranian state media reported Iran had successfully test-launched a ballistic missile with a potential 2,000-km range.[vi]	Again, under the JCPOA, Iran was forbidden to undertake any activity related to ballistic missiles designed to be capable of delivering nuclear weapons. A warhead that could be mounted on a ballistic missile is required. Estimates vary from between months and 1-2 years for development.

i IAEA Board of Governors GOV/2024/26 Date: 27 May 2024; www.iaea.org/sites/default/files/24/06/gov2024-26.pdf

ii 0. Main Text (state.gov) Signed by China, the EU Commission, France, Germany, Russia, UK and US.

iii Regarding the quantities of enriched uranium in Iran's possession and its ability to enrich them to the high level required for producing a nuclear bomb, according to the analysis of a leading American institute in the field, the Institute for Science and International Security (ISIS), within a month of deciding to begin enriching to military levels, Iran could produce enough enriched material for eight nuclear devices, within two months for ten devices, and within three months for twelve devices., INSS Insight No. 1868, June 23, 2024. Data from the IAEA indicates that, since August 2024, Iran has accumulated 17.6 km of 60% enriched uranium, for a total of 182.3 kg. This is the equivalent of four nuclear bombs, with nuclear weapons requiring uranium enriched to about 85% or higher.

iv www.aljazeera.com/news/2023/2/20/iran-denies-enriching-uranium-to-84-percent-purity-amid-iaea-row

v IAEA Board of Governors GOV/2024/26 Date: 27 May 2024; www.iaea.org/sites/default/files/24/06/gov2024-26.pdf

vi Iran says it has successfully test-launched ballistic missile, Reuters, May 25, 2023.

The clock is ticking

October 2025 was the de facto deadline for the conclusion of a follow-on agreement to the JCPoA, after which the ability of the signatories to reimpose international sanctions via the 2015 nuclear deal would expire. Technically, Iran's nuclear programme would be removed from the UN Security Council's agenda. In effect, this will mean accepting the Iranian status quo, which is nearing nuclear threshold.What is often overlooked in signatory capitals as well, is the significant milestone reached on 18 October 2023 (Transition Day) when all remaining nuclear-related sanctions against Iran under UN Security Council Resolution 2231, including restrictions on ballistic missiles and sensitive technologies, expired[14]. Technically, under the terms of the JCPOA, all previous UN sanctions related to Iran's nuclear programme can be re-imposed in the event of "significant non-performance by Iran of JCPOA commitments" (the snapback provisions). In a positive step,

14 main.un.org/securitycouncil/en/content/2231/background

in September 2023, the E3 confirmed they are "committed to preventing Iran from developing nuclear weapons, including through the snapback process if necessary[15]".

Many commentators assert that the unravelling of the JCPoA was entirely due to the then US President, Donald Trump, pulling out of the agreement in May 2018. Hitherto, Iran had seemingly fully complied with the terms of the JCPoA. From 8 May 2019 onwards Iran stopped implementing its nuclear-related commitments under the JCPOA on a step-by-step basis until, on 23 February 2021, it stopped implementing them altogether. As far as the Iranian Regime was concerned, this US withdrawal gave it the 'green light' to renege on the terms of the JCPoA, even though none of the other signatories took the US route.
It is possible Iran always intended to repudiate the main terms of the JCPoA, but this US disengagement certainly gave Iran, in its eyes, 'legitimacy'.

As the Director–General of the IAEA wrote in the latest report in November 2024, "This has seriously affected the Agency's JCPOA-related verification and monitoring activities. The situation was exacerbated in June 2022 by Iran's decision to remove all of the Agency's JCPOA-related surveillance and monitoring equipment. As a result of not having been able to perform JCPOA-related verification and monitoring activities for more than three and a half years, the Agency has lost continuity of knowledge in relation to the production and current inventory of centrifuges, rotors and bellows, heavy water and UOC, which it will not be possible to restore."[16]

Subsequently, mixed messages were sent by the Biden administration to Iran. Entering into negotiations on resurrecting the deal, the US released $16billion worth of previously frozen assets into Iranian coffers in 2023, which included $6billion as part of a prisoner swap. In turn, the Iranian Regime made only minimal concessions, diluting a small amount of enriched uranium and slowing down enrichment. The Supreme Leader highly likely concluded that the US was weak and could be taken advantage of. Formal talks have stalled, though neither side has publicly stated they have failed, in the wake of heightened tensions in the Middle East since October 2023.

Requirement to approach more strategically

It is almost certain that neither China nor Russia want Iran to achieve nuclear weapon status, but, currently, their overriding national objectives are to undermine and frustrate any US policy in the Middle East region. The dial needs to be shifted to convince both China and Russia that it is within their national interests to properly restart negotiations with Iran. Reportedly, there is recent intelligence that Russia has given nuclear technology to Iran in exchange for ballistic missiles for the Ukranian conflict. In particular, the cost needs to be higher for China, who are now purchasing roughly one third of all Iranian oil exports at a concessional price.

Strategic Reviews and Refreshes and Threat Assessments over the past few years, on both sides of the Atlantic, have devoted scant attention to the Middle East as a region, and made only token assessments of the escalating Iranian nuclear threat.[17]

Although in the 2024 Annual Threat Assessment, the US Office of the Director of National Intelligence stated that while Iran does not appear to be currently pursuing development of a nuclear device, the nuclear activities undertaken since 2020 "better position it to produce a nuclear device, if it chooses to do so[18]". The reasons for this are ostensibly clear - the pivot of focus and resources firstly towards combating China during the 2010s onwards and then Russia/Ukraine since February 2022.

15 UK to bring UN sanctions on Iran into UK law - GOV.UK

16 IAEA Board of Governors GOV/2024/26 Date:21 Nov 2024. gov2024-61.pdf

17 Integrated Review Refresh 2023: Responding to a more contested and volatile world - GOV.UK (www.gov.uk) and 2023 Annual Threat Assessment of the U.S. Intelligence Community (dni.gov)

18 www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

Furthermore, a more muscular UK policy towards Iran has, hitherto been stymied by the risk this could pose to UK embassy staff in Tehran[19], hence the fact, for example, the Islamic Republican Guard Corps is still not proscribed and why Iranian military shipments to the Houthis pre the Gaza conflict were never intercepted.

A whole Government approach

Moving ahead, organisationally, there needs to be a whole-government approach. An FCDO Head should be appointed for a minimum of three years' tenure, to lead on and co-ordinate cross-government strategy and policy, for continuity and resilience. Working closely with the MOD and the Cabinet Office will remain pivotal. Re-prioritising intelligence collection will be an important enabler, as will assembling teams who have some foundational knowledge, at least, of Iran and the region. The centrality of the US in whatever the UK plans to do is paramount and cannot be understated. In addition, France and Germany, plus the wider EU, will be important players, so meaningful channels to achieve this will be key.

Moreover, the UK and US should not indulge in optimism bias at this critical juncture. US State Department spokesperson Matthew Miller on 10th July 2024 stressed;

> **"Obviously, if the new (Iranian) president had the authority to make steps to curtail Iran's nuclear program, to stop funding terrorism, to stop destabilising activities in the region, those would be steps that we would welcome," Miller said. "But needless to say, we don't have any expectation that that's what's likely to ensue."[20]**

It is important to reiterate that the Supreme Leader, Ali Khamenei, will make the ultimate decision as to whether to construct a fully-functioning nuclear weapon.

Consequences of Inaction

What would happen the day after if Iran became a nuclear state? Israel would almost certainly see it as an existentialist threat.

The key question is whether Iran would actually use the bomb against Israel or just keep it as a deterrent. The intelligence remains opaque as to what is Iran's ultimate objective. If Iran made the first strike, its calculus would need to include the risk of suffering significant damage to its military capabilities and critical infrastructure, plus relatively high population casualties and unrest if it were subject to retaliation by Israel and/or others. Unless intelligence can definitively answer these questions, contingency planning needs to be undertaken as to how the International Community will need to handle Iran accordingly on N-day plus 1.

Israel has frequently avowed Iran will never be allowed to become a nuclear state. It is widely assessed Israel can do nothing more than inflict limited degradation on Iran's nuclear capability through a multi-domain attack on Iran's key (known) nuclear facilities[21]. The US, though, has more recently provided Israel with the busting bunker ordnance, previously denied by President Obama, that could assist in this enterprise. This is far beyond the scale of when Israel twice acted alone to destroy its enemies' nuclear reactors - in Iraq in 1981 and in 2007 in Syria, with little retaliation. However, as part of its Operation *Days of Repentance*, in October 2024, Israel allegedly severely degraded Iranian air defences, thereby showing Iranian vulnerabilities.

Whilst the position of the new Trump Presidency towards Iran remains to be conclusively set out, a hawkish position is more likely and raises the stakes of pre-emptive US action being taken against Iranian nuclear facilities.

19 In November 2011, the UK Embassy was ransacked by an Iranian Government 'rent a mob'.

20 www.timesofisrael.com/pezeshkians-win-doesnt-change-the-fact-that-iran-is-dangerously-close-to-the-bomb/10 July 2024

21 According to a report by the Arms Control Association in Washington, Iran's nuclear programme is now too advanced and widely distributed to be effectively nullified by military action. www.armscontrol.org/blog/2024-04-16/retaliation-against-iranian-nuclear-sites-would-be-counterproductive

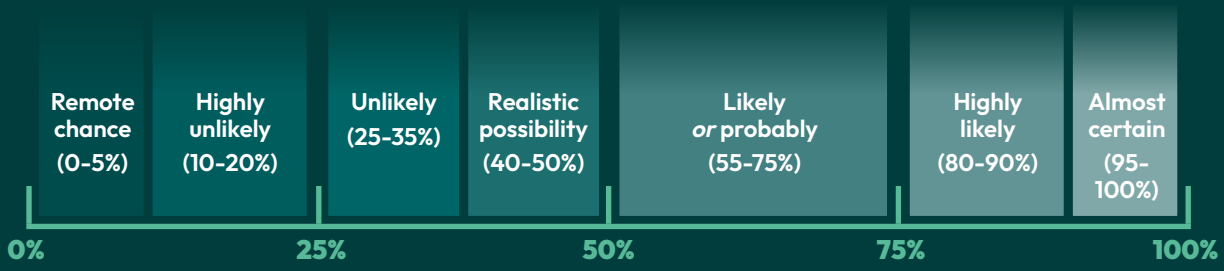
The likelihood of regional proliferation will probably be enhanced with Saudi Arabia being the most probable candidate, with Pakistan highly likely to be the main sponsor. Egypt and Turkey could be other contenders. Ultimately, Iran's possession will result in increased volatility and uncertainty in the Middle East at a time of other Great State tensions potentially accelerating.

Recommendations

The indicators are evident Iran can highly likely create a workable nuclear device. The commonly held view by UK, US and Israeli intelligence agencies is that the Supreme Leader has not made the final decision to proceed.

- Policy formulation should plan for all eventualities, including the realistic possibility Iran will have a nuclear weapon.
- The pressing nature of the looming Iranian nuclear status means that a radical review of all strategy and policy towards Iran and the region cannot wait until the Strategic Defence Review is settled. Nor should it wait long after 20th January 2025 with the new incumbent in the White House.
- Going forward, the UK must work closely with France and Germany, but, more importantly, with the US and ensure there are no divisions or surprises.
- Unpalatable as it may be, this refresh will need to consider how to bring China and Russia more fully into the negotiating arena with a full appreciation and exhortation of the levers these countries can exert on Iran.
- The lessons of the 7th October 2023 attack by Hamas in Israel must be learnt with group think and optimism bias excluded from all intelligence assessments and policy formulation. Rigorous testing should take place.
- Intelligence collection and analysis must remain a UK government high priority,and not squeezed out by perceived higher priorities. The IAEA should be provided with high classification intelligence assessments.

Probabilistic language has been used in this report, based on the Probabilistic Yardstick, a tool created by the Professional Head of Intelligence Analysis (PHIA), in the UK government, to standardise the way in which we describe probability in intelligence assessments, but it has been adopted more widely across the UK government. For example, if the term 'likely' is used, there is 'a 55-75% chance'.



How can the UK defence sector successfully adopt AI at scale?

Professor Alan W. Brown

In the last 30 years, nothing has quite captured the imagination – and anxiety – of business leaders, technologists, and the public like artificial intelligence (AI). In recent years, we have seen AI emerge from the shadows as a transformative force, promising to revolutionise business practices and drive significant economic benefits. However, when technology leaders' wild (if unsurprising) claims are supported by economists, social commentators, and politicians, then it is time to sit up and take note.

This rush to take advantage of AI's potential has spread to the whole of the defence apparatus - the MOD, the Armed Forces, and defence industry. Over several decades we have seen widespread deployment of digital technologies in many areas of defence. In the past few years, this has included a growing number of AI capabilities. The UK Defence AI Playbook[22], issued in January 2024, highlights a wide cross section of current uses of AI, from enhanced object detection in satellite images to predicting equipment failure to optimise the management of spare parts. AI is even acknowledged as playing a part in collating the Strategic Defence Review.

Deployment of digital technologies is already having significant impact in ongoing military conflicts. Activities in Ukraine, for example, highlight how digital technologies are embedded in every aspect of defence, with AI increasingly influential. Indeed, the conflict in Ukraine has even been described as "a living lab for AI warfare"[23].

Yet, despite the enthusiasm from AI advocates, a troubling reality with broader AI adoption is emerging. There is, within some quarters, a growing disconnect between the initial excitement surrounding the theory of AI's impact and the practical realities of its implementation. For example, a UK parliamentary report in January 2025 described the UK's defence AI sector as "underdeveloped" and requiring "cultivation".[24]Indeed, a commentary published in October 2024 by the Tony Blair Institute concluded that in today's AI era the UK defence strategy requires a significant reboot to be effective[25].

In this context, it is essential to ask key questions about the UK defence sector's adoption of AI at scale: Is the UK military at risk from its slow adoption of AI? Or, can the defence sector leverage AI to accelerate large-scale digital transformation?

The AI Adoption Paradox

Despite the hype and notable successes in specific areas, such as image recognition, language translation, and trend forecasting, widespread AI adoption across areas of critical operational impact face several formidable obstacles. Led by integration challenges, security concerns, and privacy issues, barriers to the cost-effective deployment of AI in complex domains such as defence are emerging.

Overcoming these barriers to broad adoption is critical in such a complex area as defence. In recent years, the UK MOD has highlighted the challenges of realising the benefits of AI across its domain. It has recognised that digital transformation of the UK defence capability is one of the most critical strategic challenges of our time. According to a 2022 policy statement[26], the UK government's goal is "to adopt and exploit AI at pace and scale, transforming Defence into an 'AI ready' organisation and delivering cutting-edge capability".

22 assets.publishing.service.gov.uk/media/65bb75fa21f73f0014e0ba51/Defence_AI_Playbook.pdf

23 www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare

24 www.janes.com/osint-insights/defence-news/air/uk-parliament-defence-committee-says-countrys-use-of-ai-in-defence-underdeveloped-mod-must-adapt-rapidly

25 institute.global/insights/geopolitics-and-security/the-uks-defence-strategy-needs-a-reboot-in-the-age-of-ai

26 www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy

The challenge, MOD has recognised, is how to achieve this goal in a diverse, complex organisation involved in a wide range of growing challenges in an uncertain world where budgetary choices have to be made. 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."**

This is a recognition that, in addition to operational issues, more fundamental questions about ethics, bias, and safety arise when deploying AI at scale in the defence sector. This leaves many people feeling trapped in a cycle of limited experimentation and unpalatable strategic choices. They struggle to identify where AI fits within their current operational constraints, who has responsibility for broad AI deployment, which policies and practices now require adjustment, and how to demonstrate AI's tangible value to its users and stakeholders.

This gap between AI's promise and its practical implementation is what I call the "*AI Adoption Paradox*".

The Two Phases of AI Adoption

To understand this paradox and chart a path forward, we need to recognise that AI adoption typically unfolds in two distinct phases.

The Experimental Phase

In this initial stage, researchers, technologists, and data scientists lead the charge, focusing on small-scale, isolated use cases. Data access might be limited, robust infrastructure services may not be in place, and quality isn't always perfect, but that's manageable at this stage – the goal here is proof of concept. Success is measured by technical performance, and funding tends to be project-based and incremental.

The Enterprise-wide Phase

Following this, broader financial, strategic, and political concerns dominate as the organisation considers the step up to large-scale, integrated systems. The focus shifts from technical novelty to strategic implementation for competitive advantage. Success criteria evolve to emphasise operational outcomes and value for money. Funding becomes strategic and continuous. Most critically, this phase demands deep integration across a variety of functions and systems, requiring a broad set of cross-functional collaboration skills to be efficient and effective.

To make progress requires a strategic approach that recognises and addresses the key barriers to delivering AI at scale – an approach that most organisations are ill-prepared to implement.

The AI Scale-Up Challenge

Moving from experimenting with AI to delivering operational improvements with AI at scale is not easy. Furthermore, in an era of rapid technology disruption, the pace of change can overwhelm organisations struggling to balance day-to-day priorities with langer-term strategic shifts. Concerns that are acknowledged as particularly acute in areas such as defence[27].

Yet, a number of key elements to delivering AI at scale are beginning to emerge. To overcome these needs, any successful approach in the defence sector will demand simultaneous progress in several key areas:

1. The Data Dilemma

Scaling AI requires a robust, accessible, and high-quality data foundation. Countless organisations struggle with data silos, inconsistencies, and privacy concerns. In the defence domain, for example, a report on the MOD's data strategy[28]concluded that despite a rising volume of data from their increasing number of sensors, they are finding it harder than ever to isolate the insight from the information. This is a major cause for concern and must be addressed rapidly if scaled adoption of AI is to succeed.

2. The Tussle for Talent

AI talent is not just about hiring data scientists – a diverse (and hard-to-find) team of AI engineers, ethicists, domain experts, and business analysts is essential. Developing existing talent and attracting new skills requires a strategic, long-term approach, which is not always a MOD strength. Finding and maintaining digital skills is acknowledged as a critical (and growing) gap in today's defence sector.[29]

3. The Culture Conundrum

Integrating AI across the enterprise requires a significant cultural shift. Building AI literacy and addressing resistance and fear across all levels of an organisation is a crucial starting point[30]. All too frequently, however, these are superficial efforts to justify management strategies without engaging sufficiently with the difficult human aspects of change management. A deeper conversation about AI's impact on individuals and teams is essential. Yet, changing the organisational culture in defence is notoriously difficult and it is acknowledged that becoming an "AI-native" defence force will require as much focus on internal reform as on technology adoption[31].

4. The Infrastructure Imperative

AI capabilities must align with a wide variety of existing systems and services. Furthermore, adapting these AI products to the military context consumes massive amounts of data in how it is trained, tuned, and applied. It demands significant computational power and advanced infrastructure to process that data in algorithms that encode complex, deep analytics. Many organisations find their legacy systems strain under the weight of AI requirements. The extent of the investment in modernising IT infrastructure to cope with these demands is always a prerequisite for AI at scale, yet often too readily overlooked in favour of other more attractive tasks. In domains such as defence, such concerns are compounded with a myriad of security and interoperability issues. Keeping the focus on infrastructure modernisation while investing in AI technology will be an important balancing act for the defence sector.

27 www.mckinsey.com/industries/aerospace-and-defense/our-insights/a-rising-wave-of-tech-disruptors-the-future-of-defense-innovation

28 www.gov.uk/government/publications/data-strategy-for-defence/data-strategy-for-defence

29 www.techuk.org/resources/3-ways-to-bridge-the-digital-skills-gap-in-uk-defence.html

30 hbr.org/2024/05/for-success-with-ai-bring-everyone-on-board

31 ukdefencejournal.org.uk/defence-committee-uk-must-learn-from-ukraine-and-embrace-ai

5. The Governance Gauntlet

The race to deploy new AI capabilities is driving rapid change, particularly in defence where the focus on competitive advantage is critical. Yet, if nothing else, the prominence of AI today has thrown down the gauntlet to leaders and decision makers everywhere – face up to the obligations of broad data-driven decision making, data collection, and digital technology management, or suffer the legal, financial, and reputational consequences.

As more intelligent systems are deployed in domains such as defence, concerns about the ethics and transparency of data and decision-making processes will heighten.

Developing a comprehensive AI governance strategy is no longer optional – it's essential. But more than that, the principles embodied in governance strategies must be a fundamental part of daily thinking and actions. How the need for security and resilience will align with this need for transparency remains an open question. Furthermore, deciding where and whether AI can act beyond being a human-focused tool and take on an autonomous decision-making role requires addressing significant issues.

6. The Technical Debt Trap

Across defence, substantial effort, time, and resource is devoted to maintaining increasingly complex technology stacks. Yet, it is tempting to launch into new AI projects without addressing underlying technical issues within existing software infrastructure with the hope that these concerns can by by-passed. Unfortunately, this is rarely the case. The accumulated "technical debt" can create significant hurdles when moving toward AI at scale. Building on this shaky foundation destabilises the robust, resilient, and reusable framework required for AI at scale delivery. Additionally, existing procurement models and very long development timescales for some defence systems handicap efforts seen in other domains to adopt fundamental shifts to agile practices across the lifecycle. Beyond the mission focus for AI, exploring use of AI to reduce the cost of managing the technical debt in defence systems is a vital task.

Responsible AI and the AI Safety Imperative

While operational concerns are at the forefront of discussions about AI adoption in defence, responsible adoption of AI technology is an equally important aspect that must be addressed. Underlying many of the challenges facing large-scale adoption of AI in defence is the unique context in which defence operates. As we push the boundaries of AI at scale in the defence sector, we cannot ignore the critical importance of AI's "three R's" – Responsibility, Reliability, and Robustness. This isn't just about preventing technical glitches – it's about ensuring our AI systems operate reliably, ethically, and in alignment with human values. There are several key considerations that dominate strategies for scaling AI adoption in these circumstances.

First and foremost is bias mitigation. AI algorithms can inadvertently perpetuate or even amplify existing biases, so it's crucial to implement rigorous testing protocols to identify and address potential biases in your AI systems. Equally important is the focus on reliability and robustness. As AI takes on more critical functions, its reliability becomes paramount. Organisations should implement comprehensive testing and validation processes, especially for AI systems involved in high-stakes decision-making.

Transparency and explainability are also vital. The "black box" nature of some AI systems can erode trust, so it's essential to strive for AI models that can be explained and understood by stakeholders, including non-technical users. Additionally, continuous monitoring and adaptation are necessary as AI systems learn and evolve. Processes should be put in place for ongoing monitoring and updating of AI systems as they ingest new data and encounter new scenarios.

Ethical frameworks play a significant role in the responsible adoption of AI at scale. Organisations should develop clear ethical guidelines for AI development and deployment that align with their values and consider broader societal impacts. Lastly, while we strive for AI autonomy in many areas, maintaining appropriate human oversight is essential, especially for critical decisions regarding collateral damage.

Appropriate ethical use of AI in defence is widely debated, and the responsibilities of leaders adopting AI at scale must be taken seriously. By addressing these key considerations, organisations can ensure that their AI systems are not only powerful and efficient but also safe, ethical and aligned with human values as they scale.

The Road Ahead: The Future of AI at scale

As we look to the future of AI, there is significant cause for optimism at the opportunities that it presents. However, we are also becoming much more deeply aware of the responsibility that adoption of AI capabilities brings.

We are on the cusp of AI systems that can dramatically enhance human capabilities, streamline complex operations, and unlock insights from vast stores of data.

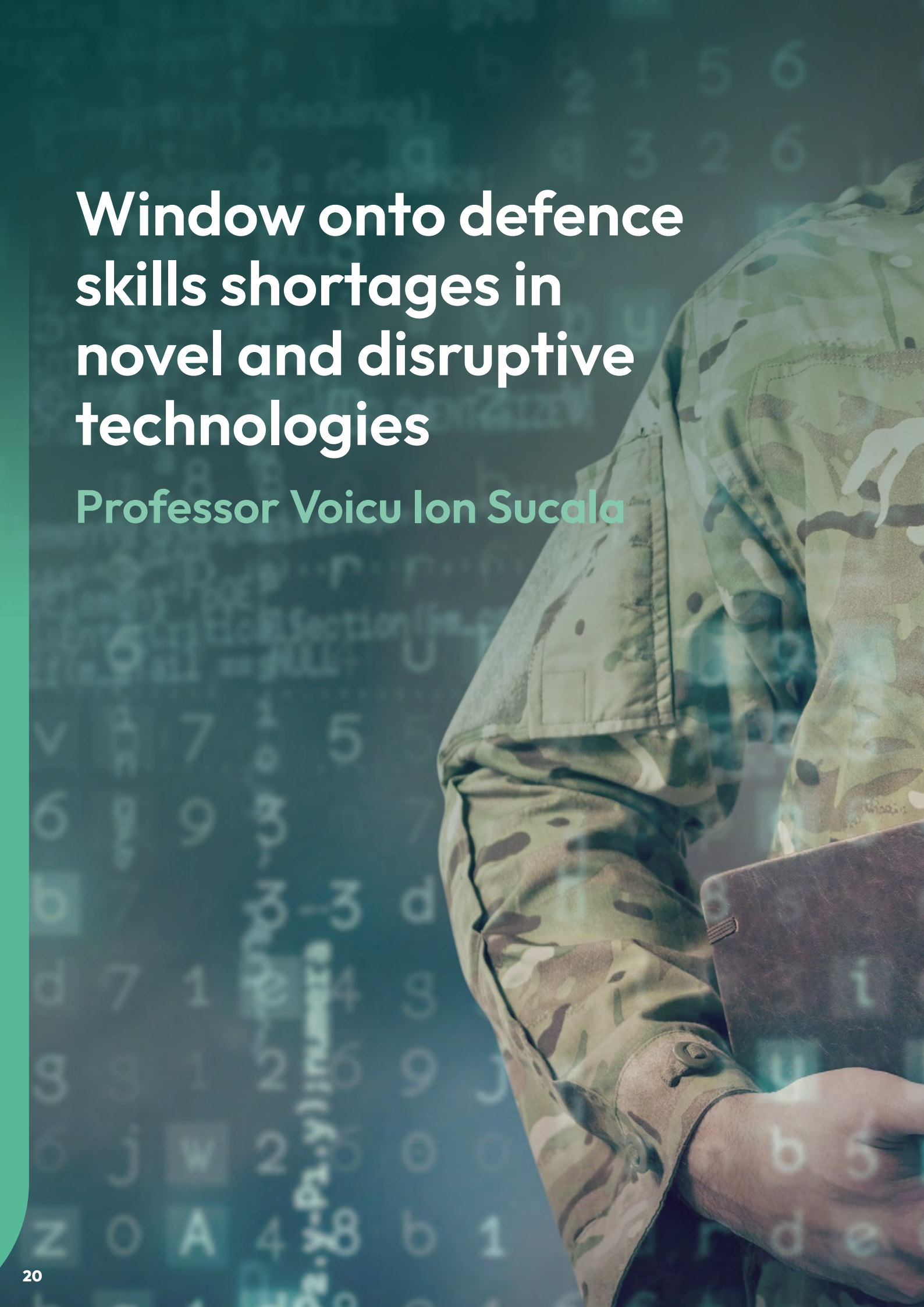
But realising this potential requires more than just technological advances. It demands a holistic approach that addresses the technical, organisational, and ethical dimensions of AI implementation in contexts that are often uncertain, ambiguous, and require balancing a variety of competing risks. As leaders, practitioners, and academics in this field, we have a duty to guide this transformation responsibly.

In domains such as defence, the challenge is even more significant. Recent reviews have found that even though our understanding of military applications and implications of AI is growing, it's still from a relatively weak foundation. Discussions often overemphasise certain high-profile concerns, such as lethal autonomous weapons systems (LAWS) while neglecting other crucial areas such as strategic planning and pre-emptive equipment maintenance. The focus on tactical issues overshadows strategic considerations. Furthermore, the short-term consequences of AI in defence often take precedence over the longer-term, additional effects that could have the most significant impact.

Hence, the path to AI at scale is not an easy one, but it is undoubtedly one of the most important journeys the defence sector must address today. By working together, sharing knowledge, and maintaining a commitment to responsible approaches, we can harness the transformative power of AI to drive meaningful change in the defence domain and more broadly across business and society.

Window onto defence skills shortages in novel and disruptive technologies

Professor Voicu Ion Sucala



Background: Significant technological developments continue to take place in the multi-domain defence space – maritime - sub and surface, air, land, space, digital and cyber. The challenge for the UK and its allies is to identify the most impactful of these technologies for deterrence, the future battlefield, peace keeping activities and the military aid to civilian authorities. Currently, in the UK, much of the debate and planning has been driven by several main factors: an ever-challenging set of financial constraints in the face of increasing spending by our main adversaries, and the lessons which need to be applied from current conflicts, most notably, in Ukraine and Middle East, plus planning ahead for new conflicts. Underpinning this is the ability to innovate at pace.

Key Technologies: In quick summary, the novel and disruptive technologies coalesce into a highly focused list: cyber and AI; quantum; robotics; energy weapons; human enhancement and space technologies. Within this list, there is a mix of areas of scientific disciplines (quantum and AI), some are physical places (space), engineering or computer science areas (robotics & automation and cybersecurity), with few unique defence 'tools' (energy weapons). The UK is considered to be strong in some areas, for example, data science and AI and advanced materials, but less so in others, for example, space.

The Problem: Several other aspects are worth highlighting while analysing the current context:

1. An acute need for engineering and technology skills, as highlighted by a plethora of government, industry and academic reports;
2. A highly permeable barrier between civil and military applications allowing for fast transfer both ways and
3. A requirement for a much-accelerated pace of innovation (from laboratory to battlefield), with an order of magnitude faster than the usual peace-time procurement cycle.

What is evident is that number 2 and 3 are highly related to the pressing skills shortages, and until they are all adequately addressed, the challenge of efficiently and effectively harnessing all defence technologies of the future, will remain sub-optimal.

Evidence Base: The evidence base for engineering and technology skills and capabilities is growing. According to the report published in 2023 by Defence Online and Guidant Global, 'the UK is experiencing a crippling shortage of science, technology, engineering and mathematics (STEM) skills' and this could result in the overall deterioration of the defence capabilities and in UK becoming 'outpaced by other countries in terms of technology'.[32] The Nuclear National Strategic Plan for Skills (2024)[33] estimates that in order to meet demand from the growing nuclear programme, at the heart of the UK's national security strategy, by the end of this decade, the UK will need to fill 40,000 new jobs, double the number of nuclear apprentices and graduates, and quadruple the number of specialist PhDs. The House of Commons report 'Developing AI capacity and expertise in UK defence' (2024-2025) acknowledges that AI has the potential to transform defence in fundamental ways but recruiting and retaining talent is a key challenge.[34]

32 UK's defence sector and STEM skills shortages | Guidant
33 NSDG-National-Nuclear-Strategic-Plan-For-Skills.pdf
34 Developing AI capacity and expertise in UK defence

What is insufficiently clarified though is that the demand isn't only quantitative – more engineers, data scientists and project managers, but also qualitatively different – employees able to explore, innovate, prototype, test and scale up at an order of magnitude at higher speed. Furthermore, future personnel should be able to use all modern tools available (e.g. generative AI) to enhance and speed up creativity and innovation.

The Solution: The UK education system is in an excellent place to deliver, providing world class graduates, with a long-standing track record. This is evident just by looking at the international demand for British higher education or by looking at international rankings – the UK has three universities in the top 10, nine in the top 100 and 20 in the top 200 (QS World University Ranking in Engineering & Technology 2024). Except for the USA, there simply isn't any other country where there is such an integrated and performing ecosystem of research and education. Another very relevant development in the last decade or so is the Degree Apprenticeship scheme, which offers access to a wide range of universities – from research intensive to local education focused, at no tuition fee.

The UK also has an excellent start-up ecosystem that ensures a smooth transfer of research results into the commercial world. Finally, despite all challenges, the research support system has a good track record, both in terms of public funding and in terms of institutional infrastructure and expertise. The Government's £20.4 billion investment in R&D planned for 2025 aims to boost innovation across the UK.[35] Commercialisation initiatives, such as the Proof of Concept Fund, Innovation Accelerators, Made Smarter Innovation Programme and the Catapult Network[36], help bridge the gap between universities and the industry.

More tailored regional strategies could further support local innovation ecosystems and the current devolution plans provide a promising perspective. The Advanced Research and Invention Agency (ARIA) launched to support high-risk, transformative research has the potential to address the gap in traditional funding models by rewarding risky ventures and fostering ground-breaking innovations that could have significant long-term benefits.[37]

All these factors, the long tradition and strong reputation of British universities all translate into a significant ability to attract top talent from all over the world, especially in the critical areas such as engineering, computer science, physics and biosciences. This is essential for a thriving and competitive R&D ecosystem and should be accompanied by the right ways to make maximum use of that talent in all research areas. However, growing local talent is essential in the defence sector, so mechanisms, such as the Degree Apprenticeship scheme, are ideal for addressing the demand at a larger scale.

Nonetheless, while our Higher Education ecosystem is comparatively good at educating large numbers of graduates in technology fields, we still face two challenges: the high cost of education, and the insufficiently modernised engineering curriculum. While it is obvious that world-class education is expensive, it is also clear that leaving graduates with significant level of debt is going to impact the quality and the volume of graduates. The Degree Apprenticeship system could provide a good solution to this challenge, grounded on closer relationship between universities and defence companies.

35 Government backs UK R&D with record £20.4 billion investment at Autumn Budget - GOV.UK

36 The Innovate UK Catapult Network provides a unique combination of cutting-edge R&D facilities and world-class technical expertise to support UK business innovation. Home - The Catapult Network

37 About ARIA

The University of Exeter's contribution: growing the skills pipeline: The University of Exeter offers world-leading R&D capabilities in areas such as advanced materials, data science and AI, autonomous vehicles, additive manufacturing, human enhancement and energy. In areas, such as metamaterials, autonomous vehicles, data science and human enhancement Exeter has long-time collaborations with a plethora of organisations. One such example is the work with Supacat, paving the way for a green revolution in defence and off-road transport.

A hybrid electrically powered version of the All-Terrain Mobility Platform (the ATMP), one of the world's most popular, versatile and battle-proven off road military vehicles, has been developed. Already validated to successfully operate in a range of very harsh terrains, the vehicle's new technology could be exported to allied forces and translated into a range of challenging 'off-highway' uses, including emergency services, rail, marine, forestry and aerospace.

The University of Exeter continuously refines its courses and curriculum responding to employer requirements and skills needs, collaborating with industry to develop this future pipeline. We have a number of mechanisms including placements, Degree Apprenticeships, Continuing Professional Development and industrial PhD placements.

Our collaborative approach to *Degree Apprenticeships* seamlessly integrates partners and academic excellence with real-world work experience, empowering learners to thrive and organisations to prosper. We are proud to offer the largest Russell Group apprenticeship portfolio. *We partner with 400 employers and deliver training to 3,000 apprentices.* Our apprentices excel in their studies, resulting in multiple individuals receiving industry awards, and in 2024 the University of Exeter was honoured with the Multicultural Apprenticeship Award for University of the Year.

Our portfolio of programmes covers Systems Thinking, Leadership and Management, Digital, Healthcare, Finance, Accounting, Civil Engineering and Mining. All our programmes offer a University of Exeter qualification and many offer additional professional body qualifications or routes to qualifications.

In addition, the University offers several *Centres for Doctoral Training (CDTs)* that offer an industry-based approach providing students with real-world industry experience and an opportunity to meaningfully contribute to the activities of a company; these cover STEM and social science subjects. One of the most developed CDTs is the Centre for Metamaterial, Research and Innovation (CMRI) (see below), but other examples of respective doctoral training programmes span Offshore renewable energy (IDCORE); Energy transition & mineral resources; BioMed; Biosciences; Medical Mycology and Environmental Intelligence using Data Science & AI. Fundamentally, CDTs. A quite from a key sponsor reinforces the excellence of the University's CDTs.

"I really enjoy working with the Centre for Metamaterial Research and Innovation at the University of Exeter. By regularly interacting with academics and cohorts of students, we can build up understanding and working relationships that work both ways. So, rather than a linking to individuals (e.g. PhD student and/or supervisor), the link is to an evolving and communicative research group. This allows us to efficiently kick around ideas to set up work packages and research proposals (to match funding opportunities that come our way)."

Dr James Dalley, Lead Engineer at Leonardo UK, Luton

CDT Example: Centre for Metamaterial, Research and Innovation (CMRI)

The CMRI is a community of academic, industrial, and government partners that harnesses research excellence from theory to application, and enables simulation, measurement, and fabrication of metamaterials and metamaterial-based devices.[38]

Our breadth is our strength: we are uniquely positioned to solve multi-faceted research questions and industry challenges. Our academic expertise spans electromagnetism (from visible and infra-red through to THz and microwave), acoustics and fluidics. The materials we work with have wide application, e.g. imaging, sensing and spectroscopy, acoustic and RF signature reduction, energy storage and harvesting. The CDT has funded PhD industrial studentships, with sponsors including Atlas, Dstl, Leonardo, MBDA, QinetiQ and Thales.

Centre for Metamaterial Research & Innovation | Centre for Metamaterial Research and Innovation | University of Exeter

youtu.be/lW1kZPnN-cs

We realise collaborations with other consortia and University partners bring enhanced dividends. The Defence Data Research Centre (DDRC), a consortium led by the University of Exeter and including the Universities of Liverpool and Surrey, the Digital Catapult and the Defence AI Centre, and designed to focus on problems related to the use of data for AI applications.[39]

Projects undertaken include:

- Facilitating reusable datasets;
- Enabling a culture of data sharing;
- Exploration of the challenges facing contemporary organisations to provide confidential, trustworthy data;
- Data Management;
- Working with Defence Medical Services to understand the demand for AI and data-driven solutions;
- Review of the state of the art in synthetic data generation;
- Increasing AI and data literacy of stakeholders within the Defence sector and
- Data resilience.

With regard to technology exploitation, the SETsquared Partnership is a collaboration between six leading research-led universities of Bath, Bristol, Cardiff, Exeter, Southampton and Surrey. It is a business incubator with a range of programmes supporting the growth and success of ventures from delivering the first idea, raising investment, scaling to an established business, or achieving a >£100 million exit. Since launching in 2002, SETsquared has supported over 5,000 innovative, high-tech, high-growth and knowledge intensive businesses to raise £4.2bn investment and create over 15,000 jobs through high-quality business support, expertise and an extensive network of incubators, universities, programmes, investors, and advisors. More specifically, it has delivered a dedicated Defence and Security Scale-Up Programme and is currently delivering Cosmic Capital through a recent award from the UK Space Agency 'Cosmic Capital – Space South Central'.

38 A metamaterial is a 3D structure with a response or function due to collective effects of their building blocks (or meta-atoms) that is not possible to achieve conventionally with any individual constituent material (UKMMN definition 2025).

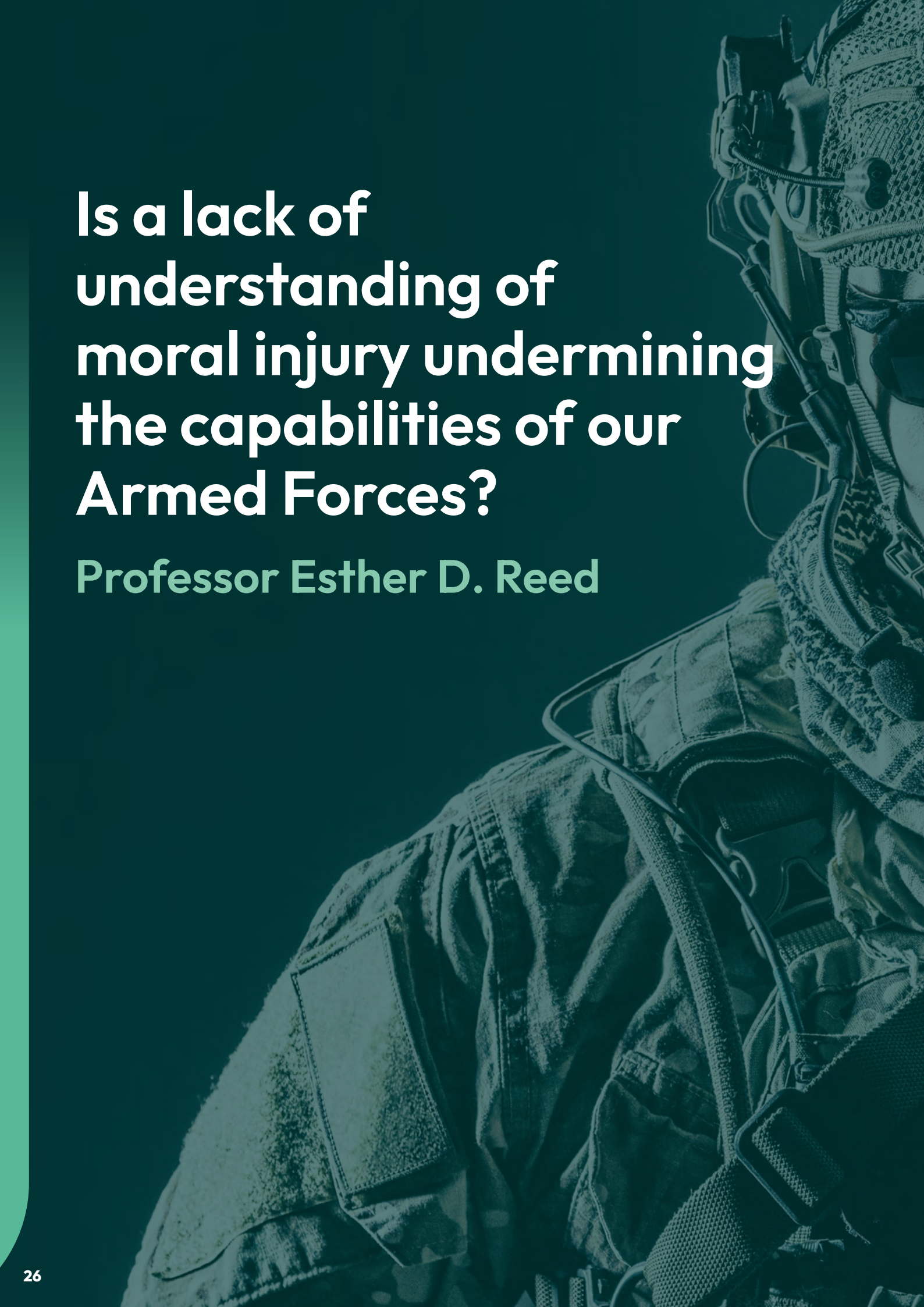
39 See Home - Defence Data Research Centre. The Centre focuses on problems related to the use of data for Artificial Intelligence applications, which can often be inaccessible or unusable in its raw state; up to 80% of time can be spent on getting data in a state where it can be used, and some projects never start at all due to insurmountable data issues.

Recommendations:

- In order to upscale the ability to generate and produce these novel and disruptive technologies at sufficient pace, sustained recognition should be accorded to the R&D ecosystem and the education system. They are the key underpinning components of this capability development.
- Enhanced partnerships between government, industry and academia with prioritisation and a sustained funding pipeline, underwritten by a whole of government strategy covering all of societal prosperity and security objectives.

Is a lack of understanding of moral injury undermining the capabilities of our Armed Forces?

Professor Esther D. Reed



UK defence personnel statistics regularly report that all three Services (Royal Navy, British Army and Royal Air Force) have below-target trained strength[40]. Personnel requirements change over the years. But below-target trained strength across all three branches of the UK Armed Forces is an undesirable situation.

A recent report on the operational readiness of the Armed Forces by the Defence Select Committee also raised concerns about retention, and welcomed the then Government's intention for a review to alleviate the crisis in both recruitment and retention.[41] UK personnel numerical strength is a critical defence consideration, with 'pinch points' presenting operational risks. It is important to establish how far moral injury is a factor in either and/or both recruitment and retention.

Moral injury is commonly defined as:

- **a betrayal of what's right**
- **by someone who holds legitimate authority (e.g. in the military – a leader)**
- **in a high-stakes situation.[42]**

Victoria Williamson, et al., write in The Lancet (Psychiatry) of moral injury as 'the strong cognitive and emotional response that can occur following events that violate a person's moral or ethical code'.[43]

How to scope the challenge?

We lack a full understanding of the extent to which moral injury is undermining defence readiness.

We know the Government aspires to train and support the Armed Forces to the highest standards. For example, the Ministry of Defence *People Health and Wellbeing Strategy 2022-2027* adopts 'an evidenced and holistic approach to health and wellbeing' that recognises the inseparability of physical and mental health, and also the moral requirement to look after the health and well-being of serving personnel.[44] Health and wellbeing are also strategic level responsibilities recognised widely as falling not only to the Chief of Defence People, Director General Defence Medical Services, but to other senior tri-service ranks. Anyone who speaks routinely with serving personnel will know that many (if not most) 'on the ground' divisional officers, career managers, chaplains, chefs and civil servants, as well as every commanding officer, recognise role(s) they have to play in reducing burnout and harmful stress-levels, mitigating mental health problems, and otherwise helping protect service personnel across the Armed Forces.

But there are gaps. Why and where are challenges not being fully understood? Where do responses fall below what's needed?

40 House of Commons Library, UK Defence Personnel Statistics by Esme Kirk-Wade (13 August 2024) researchbriefings.files.parliament.uk/documents/CBP-7930/CBP-7930.pdf at p.4 esp.

41 House of Commons Defence Committee, Ready for War? First Report of Session 2023–24. publications.parliament.uk/pa/cm5804/cmselect/cmdfence/26/report.html. Pp.30-33 esp.

42 Jonathan Shay, 'Moral Injury', Psychoanalytic Psychology (2014) Vol. 31, No.2, 182-191, at p.182. For a brief history of definitions and approaches to measurement, see Koenig HG, Al Zaben F. Moral Injury: An Increasingly Recognized and Widespread Syndrome. J Relig Health. 2021 Oct;60(5):2989-3011.

43 Victoria Williamson, et al., 'Moral injury: the effect on mental health and implications for treatment' The Lancet (Psychiatry) Comment| Volume 8, Issue 6, p.453-455, June 2021at p.453. Citing Litz BT, Stein N, Delaney E, et al. Moral injury and moral repair in war veterans: a preliminary model and intervention strategy. Clin Psychol Rev 2009; 29: 695–706.

44 Ministry of Defence, Defence People Health and Wellbeing Strategy 2022-2027 assets.publishing.service.gov.uk/media/62b3333dd3bf7f0af6480740/Defence_People_Health_and_Wellbeing_Strategy.pdf at Foreword and p.5 esp.

Why should we have a focus on moral injury?

In 2022, members of the Five Eyes Mental Health Research and Innovation Collaborative spoke about the need to integrate evidence-informed moral injury prevention into military leadership training and mission command.[45] The Collaborative understood moral injury to refer to

> **'the enduring psychosocial, spiritual or ethical harms that can result from exposure to high-stakes events that strongly clash with one's moral beliefs', and spoke inter alia of 'a pressing need for further research' to advance understanding, 'to provide guidance on the design, implementation and evaluation of moral injury interventions in the military, and more'.**

There is scope to widen this imperative to include bystanders who see moral injury resulting from the treatment of individuals, including inappropriate behaviour, miscarriages of justice and more, so that such injury is not an operational issue. Measures that prevent moral injury, especially in understanding teamwork, are a focus of research at the University of Exeter.[46] The King's Centre for Military Health Research (KCMHR), King's College London, has been for several years a UK civilian centre of excellence for military health research.[47] The Durham University International Centre for Moral Injury is robustly multi-disciplinary in its approach.[48] In other words, moral injury is robustly evidenced as a phenomenon for an unquantifiable number of military personnel. Despite significant advances in moral injury research over recent years many gaps in understanding remain. There is work to do across moral injury anticipation, scope, prevention, endurance and recovery.

This observation is supported in early-mid 2020s literature that draws upon Ukrainian experience(s). A recent study of the Ukrainian psychological recovery programme recognised the negative impact on psychological recovery and resilience of ethical factors, 'violations of the moral and communicative, motivational and volitional, value and behavioural spheres of the personality'.[49] The Ukrainian Government's official website of the Ukraine war was similarly clear about the integration needed with respect to moral and psychological support, alongside pastoral care, and meeting spiritual and/or religious needs.[50]

Closer to home, and reflecting the lack of a shared understanding of moral injury, is the continuing controversy surrounding prosecutions from the Northern Ireland troubles some fifty years ago, with the Legacy and Reconciliation Act 2023 about to be repealed. In addition, there has been more recent contention about war crimes, with SAS conduct in Afghanistan coming under scrutiny.[51] The Wigston Report, HH Lyons Report and the Parliamentary Defence Committee Women in Defence reports all highlight deficiencies from top to bottom in processes, policies and cultural appreciation.

45 Phelps, A. J., Adler, A. B., Belanger, S. A. H., Bennett, C., Cramm, H., Dell, L., . . . Jetly, R. (2022). Addressing moral injury in the military. BMJ Military Health, e002128. doi:10.1136/bmjmilitary-2022-002128.

46 Schilling S, Armaou M, Morrison Z, Carding P, Bricknell M, Connelly V (2022). Understanding teamwork in rapidly deployed interprofessional teams in intensive and acute care: a systematic review of reviews. PLOS ONE, 17(8); Batka C, Schilling S, Kinsey C (2022). Examining the Positive and Negative Aspects of US Military/Contractor Bonds in the Operational Environment. Journal of Political & Military Sociology, 48(2).

47 kcmhr.org/about

48 www.durham.ac.uk/research/institutes-and-centres/moral-injury

49 Prykhodko, I., Yanina Matsehora, Olexander Kolesnichenko, Maksim Baida, Oleksandr Vasylkovskyi (2023). The Psychological Recovery Program of Ukrainian Military Personnel after Completing Combat Missions in the Russian-Ukrainian War. Československá psychologie, LXVII(6). doi:10.51561/cspsych.67.6.455.

50 Vovk, K. (2024, 12 February). "A chaplain is a part of the soul in the great army mechanism." The value and role of chaplains at the front. Retrieved from https://war.ukraine.ua/articles/and-role-of-chaplains-in-the-armed-forces-of-ukraine/#:~:text=Chaplains%20monitor%20soldiers'%20morale%2C%20conduct,the%20Orthodox%20Church%20of%20Ukraine.

51 SAS killings: How a scandal was uncovered - BBC News

What's missing?

The need for improved resilience, motivation and morale is widely recognised already as a UK defence policy consideration. Less widely recognised is the moral health of personnel. The challenge is to bridge between recruitment and retention challenges, personnel health and wellbeing strategies, and moral injury research - with a positive emphasis on moral health as integral to well-being. We must establish how well current work in supporting the moral health of personnel is supported at policy levels, with systemic consideration paid to moral injury.

Recommendations:

- Commanding officers and others with 5+ years' experience should submit evidence about how they already care or have cared for the moral health of personnel (regardless of whether the language of 'moral health' is used), and of where they perceive gaps and/or other failings in institutional systems to undermine their efforts.
- The UK should continue working closely with allies in advancing moral injury/health research.
- The UK should make explicit in policy the need to consider the moral health of serving personnel alongside performance standards, with veterans also being included.
- The UK should consider how to include moral/ethical considerations in military doctrine.

Does the public understanding of the law of armed conflict pose a major defence vulnerability?

Professor Aurel Sari

A champion of international law

The UK prides itself as a nation committed to the international rule of law. Successive governments have repeatedly reaffirmed that commitment. The Integrated Review Refresh of 2023 promised the UK would, "work to shape an open and stable international order" based on "respect for the fundamental principles of the UN Charter and international law".[52] More recently, Prime Minister Sir Keir Starmer has voiced his own belief in international law, stating that he thought it was very important, "that we keep to our commitments on international law".[53]

While the UK's adherence to international law and institutions has been articulated on many occasions, experts have pointed out that serious work remains to be done to maintain, and in some areas re-establish, the country's reputation as a stalwart defender of international law.[54] The present essay argues that some of that effort should be focused on the law of armed conflict (LOAC). Today, a gap is opening up between the rules of LOAC on the one side and the public's perception of what those rules allow. If not addressed, this gap may develop into a major vulnerability that risks constraining the Armed Forces' room for manoeuvre in future conflicts.

The law of armed conflict

LOAC is a regime of international law that governs the conduct of hostilities and various related matters during armed conflict.[55] These rules are relevant to the UK for at least two broad reasons.

First, the norms of LOAC are binding on the UK, its agencies and personnel under international and domestic law. The UK is party to the major LOAC treaties.[56] In addition, it is bound by those rules of LOAC that have acquired the status of customary international law.[57] LOAC thus serves as a regulatory framework that governs the activities of the UK Armed Forces and other public authorities during armed conflict, determining which acts of war are permissible and which prohibited.

Second, the UK sees LOAC as a key component of the international legal order and treats compliance with its standards as an essential aspect of the international rule of law. The point was put in 2019 by Lord Ahmad of Wimbledon, then Minister for International Humanitarian Law (IHL), in the following way:

> **This Government is committed to promoting and upholding the rules-based international system, and we believe that the proper implementation of, and compliance with, IHL is an important part of that system. We are proud of our strong record of IHL implementation and compliance.[58]**

52 HM Government, Integrated Review Refresh 2023: Responding to a More Contested and Volatile World (HMSO, London, 2023), 8–9.

53 Sir Keir Starmer, HC Deb (22 July 2024) vol. 752, col. 378.

54 Elizabeth Wilmshurst and Rashmin Sagoo, 'The new government must work hard to restore the UK's reputation as a champion of international law', Chatham House (18 July 2024), www.chathamhouse.org/2024/07/new-government-must-work-hard-restore-uks-reputation-champion-international-law

55 The law of armed conflict is also known as international humanitarian law. For a detailed overview, see Marco Sassòli, International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare (2nd edn, Edward Elgar, Cheltenham, 2024).

56 These include the four Geneva Conventions of 1949 and their two Additional Protocols of 1977.

57 For an authoritative, though not universally accepted, statement of these rules, see Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Customary International Humanitarian Law, Volume I: Rules (Cambridge University Press, Cambridge, 2005).

58 Foreign and Commonwealth Office, Voluntary Report on the Implementation of International Humanitarian Law (2019), 5.

The idea that emerges here is that compliance with LOAC is more than just a narrow, legalistic matter, but involves questions of principle and substantive values: upholding LOAC is right, violating it is wrong. Compliance with LOAC is, therefore, a matter of international reputation and legitimacy. As the previous Foreign Secretary, Lord Cameron, noted:

> **One of the reasons for supporting a rules-based order is that it enables you to call out other countries when they fail to live up to it.**[59]

Of course, this cuts both ways. As the cases of Baha Mousa (Iraq) and Sergeant Blackman (Afghanistan) illustrate,[60] violations of the rules can have significant political ramifications, both domestically and internationally. Respect for LOAC is thus a key component of what UK doctrine used to describe as "campaign authority".[61]

However, the link between compliance and legitimacy invites contestation. This is driven by several factors. While much of LOAC is clear, reasonable minds entertain reasonable disagreements about what specific LOAC rules may require in particular circumstances. Those circumstances themselves may be unclear and the facts are often disputed. This has a significant impact on the outcome of any legal analysis.[62] In societies committed to the rule of law, the armed forces are expected to comply with their international obligations.

Anything unlawful is not a viable course of action. This creates an incentive to appeal to legal arguments, since establishing the illegality of a particular policy or action makes further policy debate redundant.[63] Just like war is a continuation of politics, as Clausewitz says,[64] so adversaries and third parties may turn to law as a continuation of the war itself, using legal means and methods to achieve operational effects. The term lawfare, as originally understood, was meant to capture this dimension of the law.[65] Moreover, given their content and context, serious violations of LOAC rules raise elemental questions of morality. Allegations of war crimes are, therefore, highly emotive and mobilising. While none of these processes are new, they are amplified by digital information and communication technologies and the societal changes they have set in motion.[66] Today, it is much easier for a greater number of people to advance or to repeat war crimes allegations in front of a far wider audience and do so more quickly than ever before, regardless of whether they have any subject matter expertise or not. A smart phone and an opinion is all it takes.

These are powerful factors at work. As a result, it is difficult to imagine contemporary war without allegations and counter-allegations of war crimes, crimes against humanity and worse flying around, almost the minute that fighting erupts. This is not to say that *all* such allegations are baseless or cynical, but to suggest that *some* almost certainly are.

59 Lord Cameron of Chipping Norton, HL Deb (16 January 2024) vol. 835, col. 319.

60 See The Baha Mousa Public Inquiry, Report, Vol. I, HC 1452-I (HMSO, London, 2011) and R. v. Alexander Wayne Blackman [2017] EWCA Crim 190.

61 Land Warfare Development Centre, Land Operations, Army Doctrine Publication AC 71940 (Warminster, 2017), 2-2.

62 Aurel Sari, 'Facts Matter: Assessing the Al-Ahli Hospital Incident', Articles of War (19 October 2023), lieber.westpoint.edu/facts-matter-assessing-al-ahli-hospital-incident

63 The dynamic is illustrated perhaps most clearly by the debates surrounding the invasion of Iraq in 2003.

64 Carl von Clausewitz, On War (Princeton University Press, Princeton, 1976), 87.

65 See Charles J. Dunlap, Jr, 'Lawfare Today: A Perspective' (2008) 3 Yale Journal of International Affairs 146–154; Charles J. Dunlap, Jr, 'Does Lawfare Need an Apologia?' (2010) 43 Case Western Reserve Journal of International Law 121–144; Charles J Dunlap, Jr, 'Lawfare Today... and Tomorrow' (2011) 87 International Law Studies 315–326.

66 More broadly on the latter point, see Matthew Ford and Andrew Hoskins, Radical War: Data, Attention and Control in the 21st Century (Hurst, London, 2022).

Unsplash.com

Contested information, changing expectations

The ongoing conflict in Gaza has confirmed the link between legality and legitimacy. This should not come as a surprise. Questions of legality and legitimacy have featured prominently in previous rounds of conflict between Israel and its neighbours.[67] The current fighting has also brought into sharper focus a growing gap between what until now were mainstream interpretations of LOAC and new expectations of what is permissible in warfare. The point may be illustrated by comparing the UK Government's position on Gaza with some of the narratives dominating public debate.

In September 2024, the Government reviewed its arms export licencing to Israel and concluded that there was a clear risk that certain arms exports might be used to commit or facilitate serious violations of LOAC.[68] A policy paper summarising the decision-making process mentions three main factors that fed into this assessment: Israel's obligations to provide humanitarian assistance, allegations of mistreatment of detainees and the conduct of hostilities.[69] On the latter subject, the paper declares that the Government was unable to reach 'a determinative judgment on allegations regarding Israel's conduct of hostilities', citing two main reasons.[70]

First, the summary mentions the lack of reliable information, including 'specific information about intended targets and anticipated civilian harm'.[71] Access to credible information is key to making an informed judgment about compliance. Many LOAC rules are contextual in nature, in the sense that the scope of the obligations they impose depends on the circumstances. For example, civilian objects are not liable to direct attack.[72] However, civilian objects may change their status to qualify as military objectives, for instance when they are used by enemy forces, and thus lose their immunity from direct attack. The fact that a residential building has been targeted does not imply that a breach of LOAC has occurred; it depends on what the status of the building was at the time of the attack, amongst other factors. Similarly, the often-quoted proportionality rule of LOAC requires an attacking force to compare the civilian harm expected from an attack with the military advantage anticipated.[73] Whether or not the attacking force complied with the rule depends on its decision-making process at the time. Without understanding how and why certain decisions were made, and on the basis of what information, it is impossible to offer a conclusive assessment. Of course, in some circumstances, non-compliance seems highly likely or may be manifest, even without complete access to all relevant information. Nonetheless, without reliable and sufficiently comprehensive information, most assessments of LOAC compliance will be reasonable at best and entirely speculative at worst, but certainly not sufficiently robust to permit a "determinative assessment".

Second, the summary suggests that the assessment is further complicated by the fact that, "Hamas embeds itself in a tightly concentrated civilian population and in civilian infrastructure".[74] The conflict in Gaza takes place in a densely-populated urban environment against a foe that uses this terrain to its full advantage. By definition, combat in such circumstances poses significant risks to the civilian population and infrastructure. While LOAC may require adversaries to refrain from certain means and methods of warfare

67 See e.g. Matthew S. Cohen and Charles D. Freilich, 'The Delegitimization of Israel: Diplomatic Warfare, Sanctions, and Lawfare' (2015) 9 Israel Journal of Foreign Affairs 29–48.

68 David Lammy, HC Deb (2 September 2024) vol. 753, cols 37-40.

69 Foreign, Commonwealth and Development Office, 'Summary of the IHL process, decision and the factors taken into account' (2 September 2024) www.gov.uk/government/publications/summary-of-the-international-humanitarian-law-ihl-process-decision-and-the-factors-taken-into-account/summary-of-the-ihl-process-decision-and-the-factors-taken-into-account

70 Ibid.

71 Foreign, Commonwealth and Development Office (n. 23).

72 Article 48, Additional Protocol I.

73 Article 51(5)(b), Additional Protocol I.

74 Foreign, Commonwealth and Development Office (n. 23).

in urban settings, the applicable rules do not preclude military operations altogether. On the contrary, they may permit intense combat that inflicts potentially severe levels of harm. For example, it is likely that a very large number of civilian objects will qualify as military objectives, rendering them liable to direct attack. In high-tempo and high-intensity operations, it is not at all inconceivable, therefore, that a belligerent may conduct numerous individual attacks, all of which are LOAC compliant, that cause a level of destruction that is difficult to distinguish from the devastation that a campaign of indiscriminate bombardment may have caused. Whether such levels of harm are morally justifiable, politically prudent and operationally effective are important questions, but distinct from whether or not they are compatible with LOAC.

> **It is reasonable for the summary to conclude that "despite the mass casualties of the conflict, it is not possible to reach a determinative judgment about Israel's overall compliance with the rules governing the conduct of hostilities."[75]**

This careful approach stands in stark contrast with the tone, direction and content of much of the public debate on the Gaza conflict. Social media has been awash with allegations of Israeli violations of LOAC. Countless accusations have also been made by various non-governmental organisations, international institutions and by some governments. There is no denying that Israel has questions to answer. For instance, various videos circulating on social media show Israel Defense Forces (IDF) personnel engaged in what appear to be violations of LOAC.

The IDF is reported to have opened a number of investigations into alleged wrongdoing.[76] More worryingly, there is plenty of serious reporting and analysis to suggest that some of this wrongdoing is systematic.[77] Efforts to hold Israel and Israeli personnel to account are therefore entirely proper. In fact, the UK Government's inability to reach a "determinative judgment" in September 2024, though not unreasonable, may be considered overly cautious in the light of the information that was available at the time and perhaps even more so in hindsight. However, none of this alters the fact that large parts of the public discourse are either seriously misguided, jumping to conclusions not supported by the law and the facts, or are engaged in deliberate attempts to further their own agenda through dubious legal narratives. The points that LOAC permits widescale destruction in urban warfare, that the IDF has overstepped various legal boundaries and that some of the applicable legal standards have been mischaracterised in public discourse can all be true at the same time.

75 Ibid.

76 E.g. Emanuel Fabian, 'IDF opens probe into Rafah strike, says steps were taken to prevent civilian deaths', Times of Israel (27 May 2024), www.timesofisrael.com/idf-top-lawyer-says-very-grave-rafah-incident-being-investigated.

77 E.g. see Diakonia International Humanitarian Law Centre, 'Hostilities and Rampant Violence in the oPt: Legal Updates', www.diakonia.se/ihl/jerusalem/2023-2024-hostilities-escalating-violence-opt/legal-updates.

A notable feature of the public debate surrounding the Gaza conflict is the fact that a growing number of subject matter experts appear to question what were settled understandings of LOAC. For example, some legal experts have demanded that Israel comply with standards of certainty in its targeting decisions that depart entirely from the standards adopted by the UK. Others have denied the legality of using high-explosive weapons in urban environments or advanced restrictive understandings of the concept of military objectives that contradicts established international practice and conventional wisdom. In many cases, these positions have been put forward not as re-interpretations of the existing rules, but have been claimed to reflect the law as it currently stands. These expert interventions should be seen against the background of a broader trend in recent scholarship that questions various elements of settled practice, including on proportionality[78] and the definition of military objectives.[79]

Why does this matter and what to do about it?

That there is a gap between the law as it stands and certain understandings of the rules is not a new theme. Writing in 2021, Lieutenant General Charles Pede and Colonel Peter Hayden, both of the US Army Judge Advocate General's Corps, warned that a gap, "has opened between the actual content of the law as approved and enforced by sovereign States in contrast to the more aspirational 'evolution' of the law championed by scholars, interest groups, and nongovernmental organisations in an *external* drumbeat of legal commentary."[80]

Pede and Hayden warned that the US Armed Forces, themselves, were in danger of falling into this gap by conflating law with policy under the influence of two decades of counter-terrorism and counter-insurgency campaigns, thereby risking defeat against peer-adversaries in high-intensity conflicts because of their own misunderstanding of the legal framework of warfare.

One of the lessons of the Gaza conflict is that the "*external* drumbeat" described by Pede and Hayden has become more intense. That this has real implications for Israel and its allies is plain to see. But why should the UK Government care about these developments? First, there is a danger that overly restrictive understandings of LOAC which do not reflect the law as it stands become entrenched in public and expert discourse.[81] Second, such restrictive understandings may harden into expectations that are bound to be disappointed should UK forces become engaged in major conflict. Restrictive understandings may also seep into State practice and over time corrode what were considered to be settled interpretations of the law at the international level. Finally, capable State and non-State adversaries will almost certainly seek to exploit any gap between the law as it stands and more restrictive public expectations of how UK and friendly forces should conduct themselves. In short, there is a real risk that these developments could significantly constrain British forces' room for manoeuvre. In a world haunted by the spectre of large-scale conflict where international rules and institutions seem increasingly brittle, this is a luxury they can ill-afford.

78 Luigi Daniele, 'Incidentality of the Civilian Harm in International Humanitarian Law and its Contra Legem Antonyms in Recent Discourses on the Laws of War' (2024) 29 Journal of Conflict and Security Law 21–54 (arguing that proportionality requires that the number of civilians or civilian objects suffering harm must be lower than the number of military objectives directly targeted).

79 Oona A. Hathaway, Azmat Khan and Mara Redlich Revkin, 'The Dangerous Rise of "Dual-Use" Objects in War' (August 27, 2024), forthcoming in Yale Law Journal (2025), papers.ssrn.com/sol3/papers.cfm?abstract_id=4938707 (framing 'dual-use' objects as an aberration in targeting rather than as a design-feature of Article 52(2) of Additional Protocol I).

80 Charles Pede and Peter Hayden, 'The Eighteenth Gap: Preserving the Commander's Legal Maneuver Space on "Battlefield Next"' (2021) Military Review 6–21, 7.

81 It should be emphasised that overly permissive understandings of LOAC are corrosive and a source of concern too. See International Committee of the Red Cross, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Building a Culture of Compliance for IHL to Protect Humanity in Today's and Future Conflicts (Geneva, 2024), 8.

The challenge presented here is of strategic significance and hence not something that can be brushed aside. To address it, it is necessary to better understand the key features of the expectation gap that is developing: what is driving the process, what are its dynamics and what are its implications? Based on this, Defence and other departments should make a concerted effort to narrow the gap. This is likely to consist of several strands. One line of effort is to ensure that the general public, in particular key stakeholders, are better informed. While there is much work already done in this space,[82] it is unclear how effective and targeted it is. Inspiration may be taken from allied nations.[83] Another key line of effort is to assert control over the interpretation and development of LOAC. This includes treating the revision of the UK's Law of Armed Conflict Manual as a priority and making the most of the process; encouraging and assisting like-minded nations to affirm settled understandings of the law; and supporting expert institutions and communities to offer more balanced sources of commentary and information.[84] Lastly, since the factors driving the contestation of LOAC compliance are unlikely to weaken, Defence and wider government should make a genuine effort to enhance their preparedness to deal with an onslaught of hostile legal narratives that adversaries and other unfriendly actors are guaranteed to unleash on the UK to undermine its legitimacy and exploit its vulnerabilities in the event of major conflict.[85]

82 See Foreign, Commonwealth and Development Office, International humanitarian law: UK developments and activities, 2020 to 2022 (1 June 2022), www.gov.uk/government/publications/international-humanitarian-law-uk-developments-and-activities-2020-to-2022

83 E.g. in the past, the Lieber Institute for Law and Warfare at the US Military Academy ran a Military Operations Course designed for civilian subject matter experts interested in learning the basics of military operations from active duty personnel. The course covered the targeting process and included various familiarization activities, including observing live fires.

84 This might include support for and collaboration with relevant centres of excellence, such as the NATO Strategic Communications Centre of Excellence and the Helsinki Centre of Excellence for Countering Hybrid Threats, but nurturing and supporting home-grown talent and institutions should not be overlooked.

85 Here too, there is much to be gained from international collaboration and engaging with relevant efforts, such as the legal operations programme at Supreme Headquarters Allied Powers Europe, but the primary focus must be on capacity-building at home.

Towards a circular economy within the defence and security sector

Professor Fiona Charnley with Ananda Nidhi, Alexandra Lake, Georgie Hopkins, Markus Zils

The UKRI National Interdisciplinary Circular Economy Research (NICER) Programme, a £30 million investment, aims to drive the UK towards a circular economy (CE). This report, an output of the NICER CE-Hub, summarises a six-month collaboration with the Ministry of Defence (including DSTL, DE&S & UK Stratcom) to explore the benefits of adopting CE principles within the defence sector.

It highlights the potential for waste reduction, resource optimisation, and whole-system thinking in procurement and operations, leading to cost savings, increased efficiency, and enhanced supply chain resilience. The report emphasises that embracing CE principles aligns with broader defence objectives, including mission readiness and national security.

Systemic Challenges

We live in an increasingly volatile, uncertain, complex and ambiguous (VUCA) world where symptoms of economic and environmental distress are affecting supply chains, disrupting prices and creating geopolitical vulnerability. Global disruptions including the COVID-19 pandemic and the war in Ukraine have exposed the fragility of supply chains in both defence and wider industry. In defence, this vulnerability stems from years of cost-cutting and the pursuit of efficiency gains, whilst in industry, it is the result of complex and interconnected global networks. These persistent disruptions require a reassessment of strategies to build resilience and adaptability in this "new normal." As shown in Figure 1, the UK defence sector currently faces the following systemic challenges:

Figure 1. Overview of systemic challenges within defence.

Global supply chain volatility and traceability: The current "just-in-time" global supply chain is vulnerable to disruptions like natural disasters, geopolitical tensions, and climate change, as demonstrated by a recent battery shortage in defence caused by a lack of cardboard packaging. Furthermore, to meet anti-slavery obligations and avoid reputational damage, the MOD needs greater transparency and accountability in its complex international supply chains.

Decarbonisation: NATO allies, including the UK, are committed to achieving Net Zero by 2050. The MOD, responsible for half of the UK government's emissions, needs to accelerate decarbonisation efforts to keep pace with civilian advancements. This requires supporting innovation and adopting existing technologies to meet climate targets.

Energy Geopolitics: The UK is tackling its energy vulnerability by diversifying fossil fuel sources while accelerating the transition to clean energy. Caution must be exercised that the transition to green technologies does not come with more compromising strategic dependencies on other countries who could weaponise energy systems in the future.

Material Availability: Defence relies heavily on critical materials like rare earths, facing potential shortages and price volatility due to increasing demand from sectors like electric vehicles and renewable energy. This reliance creates vulnerabilities, as seen with MRI scanners dependent on Chinese rare earth magnets. The UK government is actively addressing this through measures like the Critical Minerals Strategy and the National Security & Investment Act to secure supply chains and protect national security.

Impact of Climate Change: Climate change is increasing the frequency and intensity of natural disasters and humanitarian crises, demanding more of defence as first responders. To adapt, defence must integrate climate considerations into all planning, aligning equipment and force design with a climate-changed world. This includes increased self-sufficiency on deployments to minimise reliance on local resources and protect personnel.

Legacy Systems and Infrastructure: Aging assets and infrastructure pose significant challenges for UK Defence, including reduced efficacy, increased costs, hindered digital transformation, and cybersecurity risks. Outdated inventory systems create data silos, making it difficult to track equipment. The Royal Navy, for example, has more nuclear submarines awaiting decommissioning than in active service, illustrating the strain legacy systems place on resources and capacity.

Defence operates within a complex system vulnerable to resource scarcity and climate change, with its own operations contributing to the problem. Recognising this, it's taking positive steps by integrating sustainability into financial policies, processes and controls. However more needs to be done to translate this ambition into concrete action.

Towards a Circular Economy

While renewable energy is crucial, a CE is essential to address the remaining 45% of greenhouse gas emissions by changing how we produce and consume. Unlike the extractive linear economy, a CE is regenerative, restoring resources and redefining value beyond profit. Its core principles, as defined by the Ellen MacArthur Foundation, include eliminating waste, circulating materials, regenerating nature, and relying on renewable energy. While often misinterpreted as just enhanced recycling, a CE aims to maintain resources for repeated use, as shown in figure 2. This report focuses on the technical aspect of the CE, maximising the lifespan of materials and products through strategies like repair and remanufacturing.

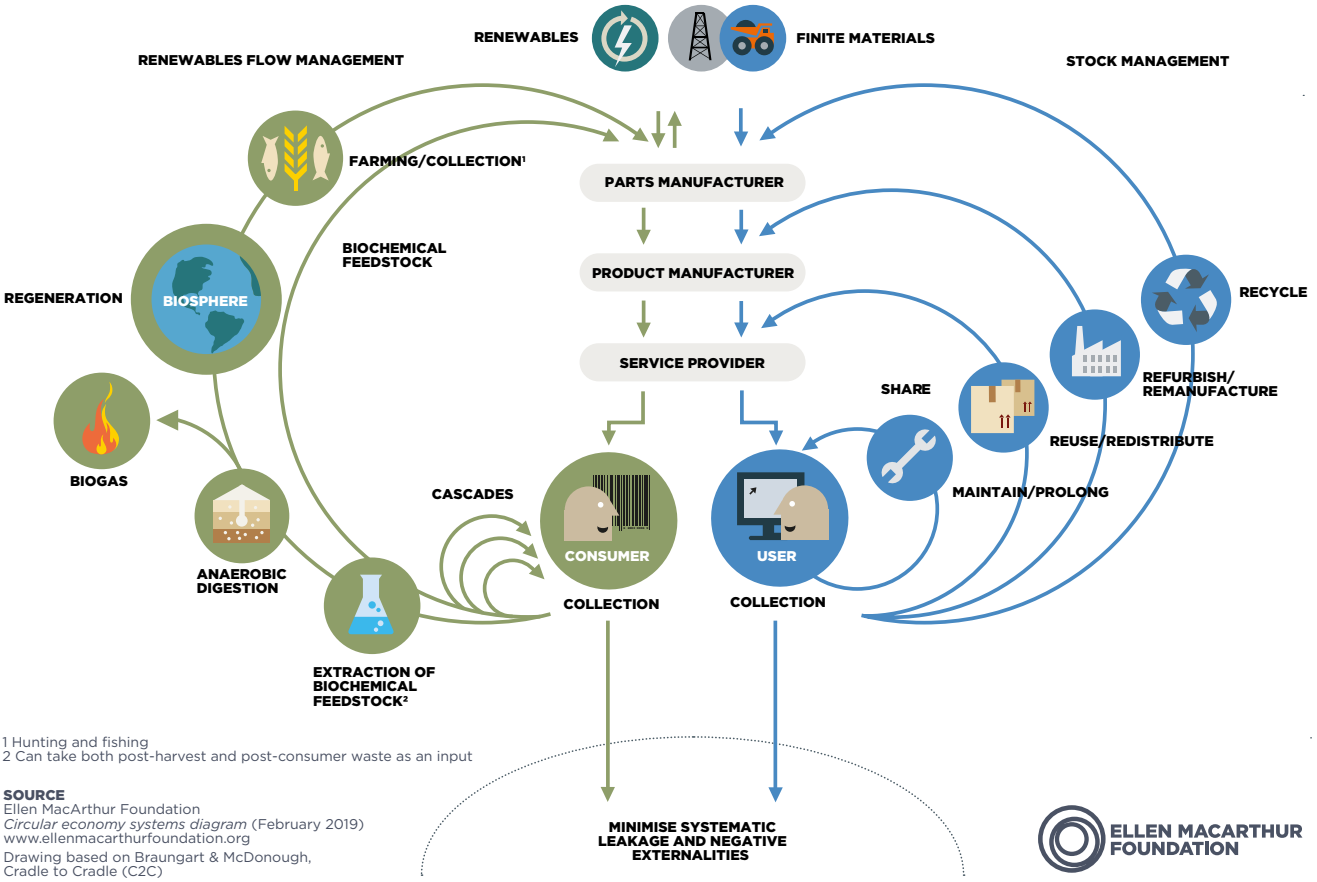


Figure 2. Circular economy system diagram (Ellen MacArthur Foundation, 2015).

Circular Economy in Practice

This section draws together examples from both defence and wider industry of circular interventions across the value chain, which can be immediately applied. Examples are categorised into three phases of a value chain: *Inflow* (acquisition and sourcing of raw materials and components), *In-Use* (use of products by businesses and consumers) and *Out-Flow* (end of life management of products and materials including disposal, recycling and recovery).

Inflow phase: reduce inflow

Workwear Procurement: In 2014, the Dutch Ministry of Defence implemented a circular procurement strategy for military workwear, requiring at least 10% recycled content. This initiative successfully stimulated innovation, with suppliers increasing the recycled content in overalls and towels to 14% and 36% respectively during the contract period.

Office Furniture: Office furniture constitutes 11% of global furniture consumption and contributes significantly to global waste. Companies like Ahrend and Rype Office are leading the way in circularity by offering furniture-as-a-service (FAAS) and remanufacturing used furniture. Rype Office has experienced significant growth, doubling revenue and staff annually, serving over 260 customers while preventing over 400 tons of waste and saving approximately 1,000 tons of CO_2e emissions, all while providing over 7,000 hours of living wage employment.

In Use phase: asset optimisation

Vehicle Life Extension: Project LURCHER, a British Army initiative, is converting diesel Land Rovers to electric vehicles (EVs) using a drop-in kit. This extends the lifespan of existing vehicles, enhances performance, and allows for comparison with diesel and hybrid equivalents. This example highlights the potential for EV technology in the defence sector, mirroring similar transitions in other public sectors like Transport Scotland's investment in electric buses.

Lighting as a Service: Schiphol Airport partnered with Signify to develop sustainable and easily replaceable and repairable lighting. These new luminaries last 75% longer, consume 50% less energy, and come with a 5-year maintenance contract. The airport benefits from reduced Total Cost of Ownership and addresses end-of-life lighting concerns by returning them to Signify for remanufacturing or recycling.

Other cases in consumer electronics and civilian jet engines provide valuable examples of product life and performance extension.

Outflow phase: post-use asset recovery

Naval platform recycling: Decommissioned in 2014, the 16,000-tonne HMS Illustrious aircraft carrier was ultimately recycled by LEYAL Ship Recycling Ltd in Turkey. Despite some equipment being repurposed, 94.06% of the vessel (13,657 tonnes) was recovered and recycled in compliance with EU and UK regulations. Similarly, Thales Group is helping the French Air Force and other NATO allies dismantle and repurpose reconnaissance pods.

Strategic Material Recovery: The U.S. military's Defence Logistics Agency (DLA) Strategic Material Recovery and Reuse Program (SMRRP) recovers vital materials like Germanium and Super-alloys from disposed parts, adding them to the National Defence Stockpile (NDS). This ensures domestic supply of crucial materials for both defence and civilian use during emergencies.

Identifying challenges to CE adoption in Defence

The following four key challenges to CE implementation have been synthesised from various stakeholder engagements including interviews and workshops.

1. **Maintaining Military Capability** remains a priority, but the adoption of a CE can be challenging due to operational requirements and complex supply chains. The focus on mission readiness often leads to new asset procurement instead of repair or reuse, and the diverse nature of military equipment makes it difficult to implement uniform CE strategies. Additionally, the need for reliable resources and the complexity of supply chains pose challenges to inventory management and the implementation of CE initiatives.
2. **Organisational Challenges:** Shifting to a CE within the MOD faces challenges rooted in its organisational structure and culture. These include risk aversion, bureaucratic inertia, siloed departments, unclear decision-making authority, and resistance to change. Additionally, competing priorities between long-term planning and immediate needs, along with a limited understanding of CE principles, further hinder progress.
3. **Inventory and Infrastructure:** Outdated inventory systems and infrastructure hinder the MOD's ability to embrace circularity. Deficient data tracking, a shortage of skilled workers and facilities, and obsolete systems make it difficult to identify opportunities for repair and reuse. This, coupled with the practice of outsourcing disposal, represents a significant barrier to implementing CE strategies.
4. **Procurement:** MOD procurement poses challenges in promoting circularity. Barriers to SME engagement, such as complex processes e.g. the need to demonstrate social value, limit innovation. Additionally, annual budgets and a lack of lifecycle perspective hinder the integration of circularity into purchasing decisions.

Towards a Circular Defence Sector

Establishing a CE in UK Defence requires strong leadership and collaboration. Progress can be envisioned in three phases, aligning with the MOD's Climate Change and Sustainability Strategic Approach. Phase 1 involves a diagnostic assessment to evaluate the current state of CE and identify opportunities. Phase 2 focuses on proving the value of CE through pilot programmes and data analysis. Selecting pilot projects for a CE in Defence requires a framework to prioritise initiatives. One approach is to categorise potential products based on inventory tiers:

1. **Permanent Inventory:** High-value, long-lasting assets like vehicles and aircraft.
2. **Intermediate Inventory:** Components and subsystems for maintaining permanent assets.
3. **Consumables Inventory:** Frequently used items with high consumption rates.

This framework helps focus on products with significant lifecycle costs and environmental impacts, ensuring that pilot projects maximise the benefits of CE principles.

Phase 3, scaling implementation, requires a comprehensive roadmap, strong leadership, dedicated resources, and specific KPIs. Lessons from Phase 2 will inform system integration and wider collaboration across government, industry, and Defence. This phased approach allows for informed decision-making and risk mitigation before full-scale implementation.

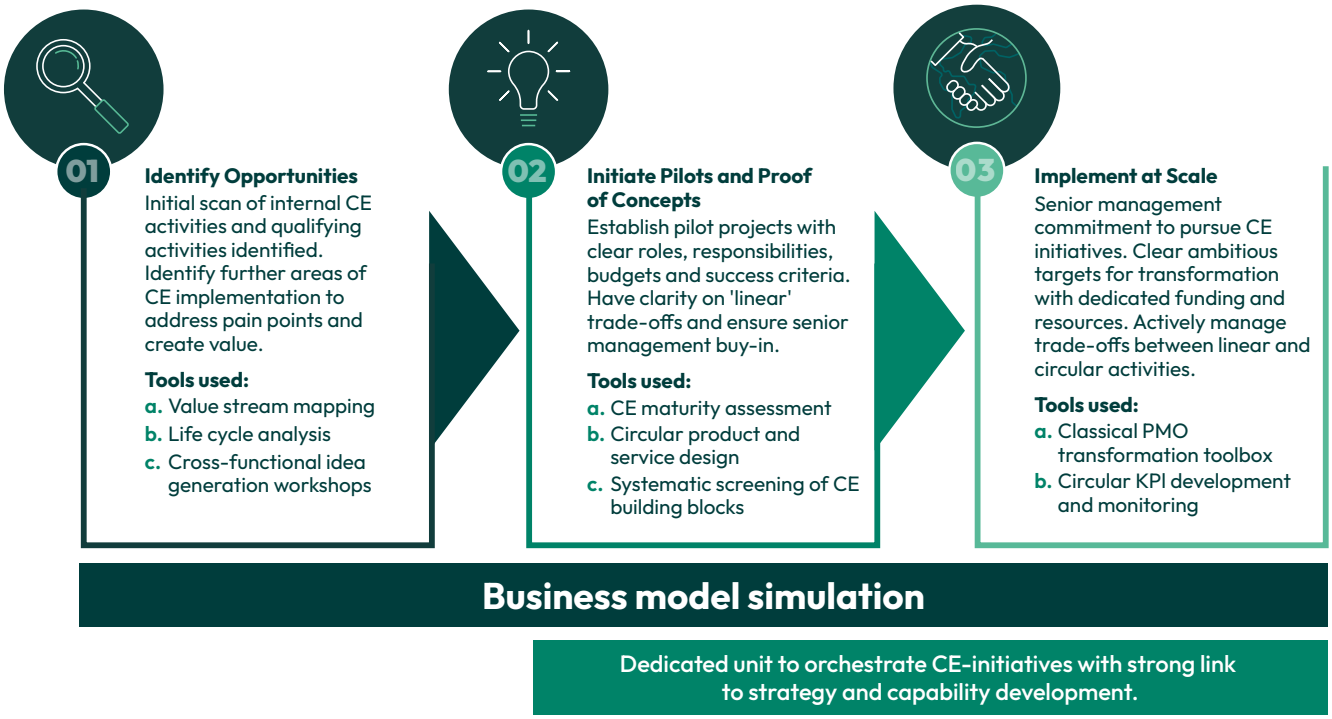


Figure 3. CE as a programmatic approach (adapted from Zils et al, 2023).

Key capabilities for adopting a CE

In practice, companies and organisations who are already benefitting from the CE typically succeed by harnessing the following core building blocks:

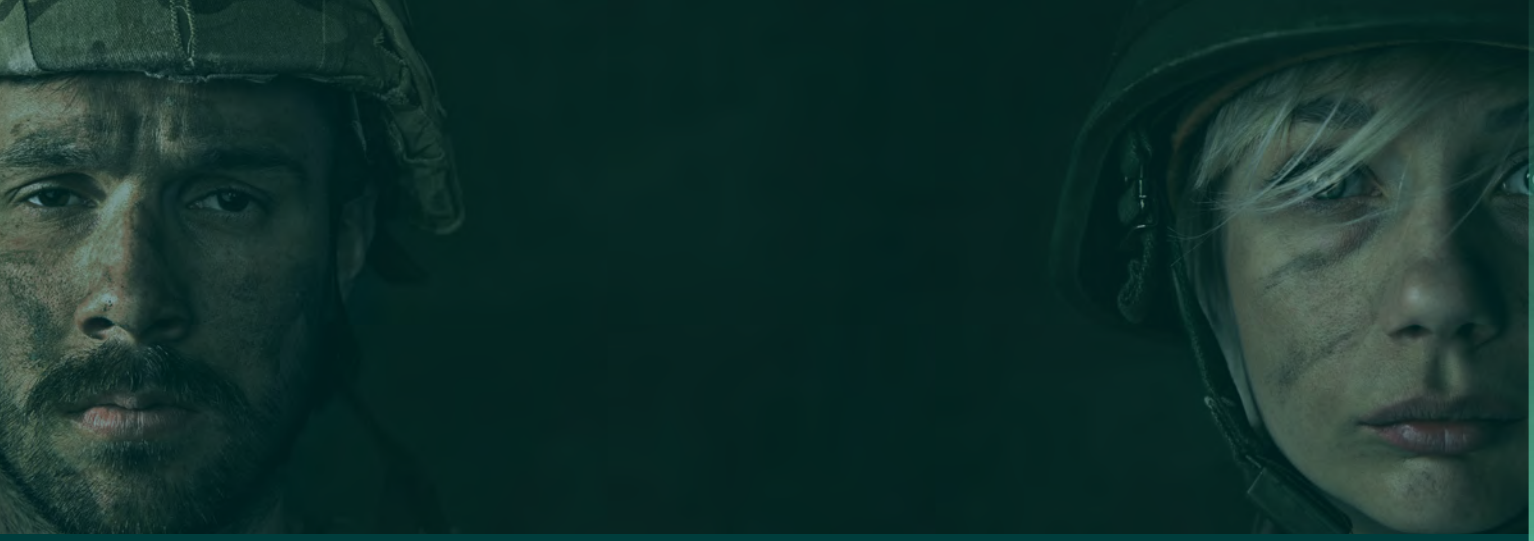
Design: Designing for a CE in defence requires collaboration across the supply chain to minimise resource consumption, reduce reliance on fossil fuels, and extend product lifespans. This involves streamlining procurement, fostering collaboration between contractors and SMEs, and integrating circularity considerations throughout the entire lifecycle. Additionally, establishing reverse logistics from the outset ensures effective resource recovery and recirculation, as demonstrated by the Dutch MOD workwear example.

Business Models: Adopting CE business models in defence means prioritising total cost of ownership and carbon footprint. This involves shifting to performance-based models, promoting product lifespan extension through upgrades and remanufacturing, and exploring collaborative initiatives like industrial symbiosis. Leasing models can be readily implemented for mature product categories such as office furniture and IT equipment.

System Enablers:
Establishing a robust system wide CE within defence requires a multifaceted approach built on six key pillars:

- **Leadership:** Strong leadership is crucial, setting a clear strategic direction and assigning responsibility for CE initiatives. Leaders must champion the transition, embedding circularity into the organisation's mission and values.
- **Workforce:** A skilled and knowledgeable workforce is essential, particularly in logistics and inventory management. This involves addressing staffing pressures and ensuring the MOD has the right skills to implement IT-enabled transformation programmes for managing inventory effectively.
- **Education:** Educating stakeholders across the value chain – including users, industry partners, and suppliers – is vital. Raising awareness about CE principles and benefits, and how they address Defence-specific challenges like resource scarcity, will foster understanding and buy-in. This can be achieved through training programmes, workshops, and awareness campaigns.
- **Behaviour Change:** Shifting to a CE requires overcoming inertia and driving behaviour change within a traditionally hierarchical institution. This involves cultivating a culture of innovation, collaboration, and continuous improvement, supported by effective communication strategies to engage employees and stakeholders.
- **Data:** Access to accurate, timely, and interoperable data is critical for informed decision-making and optimising CE initiatives. This includes data on resource flows, material usage, lifecycle impacts, and performance metrics. Robust data management systems, potentially leveraging technologies like the Internet of Things (IoT) and blockchain, are needed to improve visibility and traceability throughout the supply chain.
- **Finance:** Aligning financial incentives with CE goals is crucial. This involves directing investments towards defence firms that prioritise sustainability and adhere to ESG (Environmental, Social, and Governance) frameworks. This encourages initiatives like resource reduction, waste minimisation, and sustainable practices throughout the supply chain.

By addressing these six pillars, defence can create a strong foundation for successful CE adoption and implementation, driving innovation, sustainability, and resilience across its operations and supply chains.



Conclusions

This report highlights how a circular economy (CE) offers a comprehensive solution to challenges faced by the Ministry of Defence, from resource scarcity to environmental impact. By embracing CE principles, defence can enhance efficiency, reduce costs, and contribute to net-zero targets. Strong leadership, education, and a shift in organisational culture are crucial for successful implementation and a more sustainable future.

Next Steps

The transition to a circular economy requires collaborative knowledge sharing. The CE-Hub and Exeter Centre for the Circular Economy support this through various initiatives:

- **Networking & Knowledge Sharing:** Fostering dialogue and innovation through workshops and engagement with national and global networks.
- **Circular Economy Masterclass:** A 6-week online programme providing in-depth knowledge on CE principles and implementation.
- **Circular Procurement Masterclass:** A 4-week online programme focusing on circular procurement and supply chain management.
- **Bespoke Education:** Tailored workshops addressing specific organisational challenges.
- **Corporate Consultancy:** Providing access to academic expertise and research support.
- **Knowledge Transfer Partnerships:** Facilitating collaborative projects between businesses and academia.
- **Graduate Internships:** Bridging the gap between education and industry.
- **MBA Consultancy Projects:** Leveraging student expertise to address real-world business challenges.

These activities aim to equip organisations with the necessary tools and knowledge for successful CE implementation.

References:

Charnley et al., (2024) Engaging with Defence and Security on the Circular Economy Position Paper. Available at: Engaging with Defence and Security on the Circular Economy - CE Hub

Defence Support Futures. (2023, October 25). Circular Defence. Workshop – Challenge and Insight to Inform Circular Economic Concept Note, Bristol, United Kingdom of Great Britain and Northern Ireland. www.teamdefence.info/event/susdefsp-swg-circular- economic-concep

Zils, M., Hopkinson, P., Charnley, F., Pencheon, D.,Dawson, T., Eatherley, D., Burton, K., Gopfert, A. (2021) 'Accelerating the transition towards a net zero NHS'. University of Exeter Centre for Circular Economy, in association with Philips UKI. Available at: ce-hub.org/knowledge-hubaccelerating-the-transition- towards-a-net-zero-nhs

What impact will climate change have on military operations and readiness?

Dr Jesse F. Abrams

The world is currently facing an unprecedented convergence of climate change impacts, resource scarcity and geopolitical tensions. These are not future problems - the impacts of climate change are already outpacing predictions, with a significant increase in the frequency and severity of extreme climate events over the past decade. Global mean temperatures have already reached 1.3°C above pre-industrial levels, while 2024 was the hottest year ever and the first year to break 1.5°C.

In the UK, rising global temperatures translate to heavier rainfall, flooding, heatwaves, and storm surges along the coast.[86,87] This leads to impacts on military assets, operations, supply chains, and personnel that are vulnerable to such extreme weather. Simultaneously, armed forces are increasingly expected to support responses to climate-related disasters and humanitarian crises, putting further stress on resources and capacity.[88]

The UK MOD has taken steps by recognising climate change as a security issue and developing a strategy to help the military adapt to and mitigate the effects of climate change.

This essay reflects upon the current state of UK defence thinking on climate change, focusing on the threat that extreme events associated with climate change present, highlighting the underestimation of its impacts.

Current understanding of the impact of climate change on UK Defence and National Security

The UK defence and national security community broadly recognise climate change as a dominant global trend and risk multiplier. There is a general awareness of the threats to UK military infrastructure, personnel, and operations both at home and abroad, with a growing recognition of the direct impacts of extreme weather on military assets and capabilities. There is recognition of climate as a stress multiplier and the potential role it will play in geopolitics,[89,90] acknowledging how climate impacts can exacerbate existing tensions, create new security challenges, and is a risk to vulnerable populations. We have already seen a shift in the military's role, and anticipate a continued increase, towards the need for military assistance and stability operations in response to climate-related crises and disasters. These issues are broadly understood in the MOD's current approach to climate security; however, it does not fully capture the urgency and complexity of the challenge.

Impacts on domestic military infrastructure, personnel, and operations

There is an increasing risk from extreme weather hazards to UK-based military infrastructure and assets. Coastal navy bases are vulnerable to rising sea levels and storm surges while inland army bases, and air stations are at risk from more frequent occurrence and increased severity of river flooding. More frequent and severe heatwaves also threaten military assets, operations and personnel. In July 2022, the runways warped and melted under extreme heat during the record-breaking heatwave which saw temperatures exceed 40°C for the first time in the UK causing flights to be disrupted.[91] In the summer of 2024, a Guardsman very publicly passed out during rehearsal exercises.[92]

86 Kendon, M., McCarthy, M., Jevrejeva, S., Matthews, A., & Legg, T. (2019). State of the UK climate 2018. Int. J. Climatol, 39(Suppl 1), 1-55.
87 Committee on Climate Change (2022). UK Climate Change Risk Assessment 2022.
88 Ministry of Defence (2021). Climate Change and Sustainability Strategic Approach.
89 climateandsecurity.org/2023/01/briefer-climate-change-as-a-threat-multiplier-history-uses-and-future-of-the-concept
90 Scheffran, J., & Battaglini, A. (2011). Climate and conflicts: the security risks of global warming. Regional Environmental Change, 11, 27-39.
91 www.reuters.com/world/uk/uk-royal-air-force-halts-flights-base-heatwave-melts-runway-sky-2022-07-18
92 www.bbc.co.uk/news/articles/c1eee28w58ko

Additionally, prolonged heat puts stress on temperature-sensitive equipment such as aircraft, vehicles and radar systems and increases cooling costs for buildings and information technology systems. Extreme weather also has the potential to disrupt military operations and increase costs thereof. Heavy rainfall and flooding impede mobility, destroys vehicles and equipment, and disrupts supply routes. During the floods in Somerset in 2014, the Army had to deploy specialist vehicles to navigate flooded roads and rescue stranded residents.[93]

Extreme weather also threatens the civilian infrastructure upon which the military relies, such as electricity grids, transportation networks and communication systems.[94,95]

For instance, in 2014, the collapse of the railway line at Dawlish due to coastal storm damage cut off rail access to the naval dockyard at Devonport for two months.[96]

Further - as we saw during the 2022 heatwave - high temperatures cause rail tracks to buckle and overhead power lines to sag, leading to speed restrictions and service disruptions that can delay transportation. Compounding these risks, much of the UK military's infrastructure and building stock is ageing and was not designed with climate resilience in mind. Older buildings and infrastructure are more susceptible to weather damage, and are also costly to retrofit. According to the National Audit Office, in 2021 40% of the Defence Estate was over 50 years old, and the maintenance backlog has risen above £4 billion.[97] These make military infrastructures vulnerable to disruption and degradation from extreme weather.

Impacts on military infrastructure, personnel, and operations abroad

While the direct impacts of extreme weather on UK domestic military infrastructure and operations are very important, the consequences of climate change overseas could prove to be even more disruptive to UK defence and security interests. The UK has a global military footprint, with bases, training areas, and operational deployments in several regions highly exposed to climate-related risks, including the Middle East, South Asia, and the Caribbean. The UK has a significant military presence in the Middle East, which is a region that is particularly vulnerable to climate change impacts. RAF Akrotiri, in Cyprus, serves as a key operational hub in the region and plays an important role in the operation of the vital SIGINT (Signals Intelligence) radar in the Troodos Mountains. This facility is highly vulnerable to climate-related events with an increasing risk of severe weather and major risk stemming from rising sea levels.[98] This could have serious implications for UK intelligence gathering and strategic operations in the region. Elsewhere, the operational headquarters of the RAF in the Persian Gulf is in Qatar and other facilities in the UAE and Oman face challenges from the increasing occurrence of extreme heat and potential water scarcity issues.

93 www.independent.co.uk/news/uk/home-news/uk-floods-army-deployed-to-somerset-levels-as-military-planners-and-specialist-vehicles-provide-support-to-victims-9094223.html

94 Dumas, M., Kc, B., & Cunliff, C. I. (2019). Extreme weather and climate vulnerabilities of the electric grid: A summary of environmental sensitivity quantification methods (No. ORNL/TM-2019/1252). Oak Ridge National Lab.(ORNL), Oak Ridge, TN (United States).

95 www.bsr.org/en/emerging-issues/infrastructure-breaks-under-extreme-heat

96 Dawson, D., et al. (2016). Sea-level rise impacts on transport infrastructure: The notorious case of the coastal railway line at Dawlish, England. Journal of Transport Geography, 51, 97-109.

97 www.nao.org.uk/wp-content/uploads/2021/06/Optimising-the-defence-estate.pdf

98 Hochman, A., Marra, F., Messori, G., Pinto, J. G., Raveh-Rubin, S., Yosef, Y., & Zittis, G. (2022). Extreme weather and societal impacts in the eastern Mediterranean. Earth System Dynamics, 13(2), 749-777.

Difficult conditions in many operational theatres accelerate wear and tear on equipment, requiring more frequent maintenance and replacement. Heatwaves can reduce aircraft range and effectiveness by limiting their payloads and flight times[99], rough seas and high winds can interfere with naval manoeuvres and flight operations from carriers[100], and physical changes to the environment such flooding or storm damage can impact access of personnel. The UK military had first-hand experience of these challenges during relief operations after Hurricanes Irma and Maria in the Caribbean in 2017[101]. The widespread flooding, debris, and power outages affected ground movements and communications, while the hot and humid conditions strained personnel.[102]

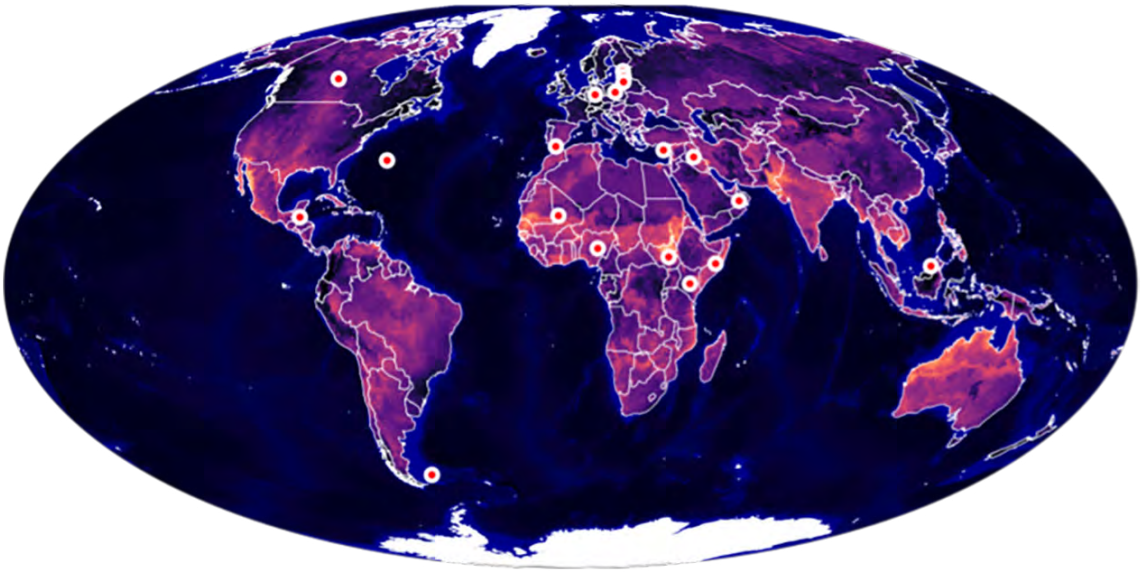


Figure 1. UK military bases abroad plotted on top of a combined future extreme event hazard layer. The hazard layer indicates the likelihood of exposure to extreme events in 2030 - higher likelihood is indicated by brighter colours (yellow), while lower likelihood areas are darker (black).

Shifting Geopolitics and Climate Change as a Stress Multiplier

Climate change has the potential to reshape geopolitics and alter the UK's strategic interests – affecting different regions in distinct ways. Climate change exacerbates existing issues in many contexts – driving conflict, the involuntary displacement of people, resource scarcity and other human security issues.

Climate change may drive competition for control and access to resources to new regions. In the Arctic, retreating sea ice is opening new shipping routes and intensifying competition for resources.[103] The UK, as a "near-Arctic state," has strategic interests that could be affected by these changes. Extreme weather events, unpredictable ice conditions, and thawing permafrost could impact potential UK operations or partnerships in the region.

99 Coffel, E. D., Thompson, T. R., & Horton, R. M. (2017). The impacts of rising temperatures on aircraft takeoff performance. Climatic change, 144, 381-388.

100 Jing, Q., Sasa, K., Chen, C., Yin, Y., Yasukawa, H., & Terada, D. (2021). Analysis of ship maneuvering difficulties under severe weather based on onboard measurements and realistic simulation of ocean environment. Ocean engineering, 221, 108524.

101 news.sky.com/story/uk-ill-prepared-to-help-after-hurricanes-irma-and-maria-devastated-caribbean-11279018

102 https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/722/722.pdf

103 Melia, N., Haines, K., & Hawkins, E. (2016). Sea ice decline and 21st century trans-Arctic shipping routes. Geophysical Research Letters, 43(18), 9720-9728.

Regions already affected by conflict and crisis are more likely to be overwhelmed by the effects of climate change. The Middle East and North Africa, already marked by political tensions and resource scarcity, face increased risks of conflict and displacement of populations due to climate change[104]. Severe droughts could lead to crop failures and water shortages, potentially triggering mass migration, urban unrest, and heightened competition for limited resources. The Syrian civil war, while complex in its origins, was partly fuelled by such climate-induced stresses.

Large scale shifts in temperature and precipitation patterns may fuel existing tensions. In South Asia, changing monsoon patterns and glacial melt in the Himalayas threaten devastating floods and long-term water scarcity[105]. This may intensify long-standing tensions between nuclear-armed India and Pakistan over shared river systems. The region's vulnerability to climate change and its potential impact on stability and security was highlighted by the 2022 record flooding in Pakistan, which affected over 33 million people[106].

The Underestimation of Climate Risks

The previous section highlighted the landscape of risks due to climate extremes that the UK defence establishment acknowledges in some form. However, both the UK and international allies defence planning, have significantly underestimated the scale, pace, and complexity of the climate security challenge[107,108]. Current thinking often views climate change as a long-term, gradual, first-order issue. However, the reality is that climate change is already a key driver of insecurity, with impacts being felt now rather than in some distant future.

The defence sector has yet to fully grasp how drastically conditions are likely to change and how quickly these changes may occur. The manifestation of impacts from climate change are outpacing scientists' predictions in both frequency and intensity. Furthermore, current assessments often fail to account for the potential of nonlinear change (such as tipping points), cascading effects, and compound risks that could rapidly accelerate the pace of change and magnify its impacts. These threats are escalating with an increasing chance of triggering tipping points this century. This has led to a significant underestimation of the threat that climate change poses.

In our recent report[109] we demonstrate how tipping points in the Atlantic Ocean circulation, specifically the collapse of the subpolar gyre, could cause shocks to the UK food, energy and economic systems. We show that there is a non-negligible chance of this tipping point being triggered as soon as 2040 and a 45% of it being triggered this century. The UK is particularly vulnerable to tipping points in the Atlantic Ocean due to its geographic location and would be amongst the countries worst affected by the North Atlantic Subpolar Gyre (SPG) collapse. However, the UK is not prepared for this event and tipping points (as well as other climate change threats) do not even appear on the national risk register.

104 Sowers, J., Vengosh, A., & Weinthal, E. (2011). Climate change, water resources, and the politics of adaptation in the Middle East and North Africa. Climatic Change, 104(3), 599-627.

105 Immerzeel, W. W., Lutz, A. F., Andrade, M., Bahl, A., Biemans, H., Bolch, T., ... & Baillie, J. E. M. (2020). Importance and vulnerability of the world's water towers. Nature, 577(7790), 364-369.

106 www.independent.co.uk/climate-change/news/pakistan-floods-cause-climate-change-b2168119.html

107 publications.parliament.uk/pa/cm5804/cmselect/cmdfence/32/report.html

108 Burnett, M., & Mach, K. J. (2021). A "precariously unprepared" Pentagon? Climate security beliefs and decision-making in the US military. Global Environmental Change, 70, 102345.

109 www.ippr.org/articles/security-blind-spot

Figure 2. Satellite image of Hurricane Ernesto as it barrels toward Bermuda. This image illustrates the increasing threat of intense tropical cyclones. Climate change is projected to enhance hurricane intensity, with potential for more Category 4 and 5 storms. This trend poses significant challenges for UK defence, necessitating increased preparedness for humanitarian assistance and disaster relief operations in affected overseas territories and partner nations. The intensification of hurricanes also underscores the need for climate-resilient infrastructure in strategic locations and adaptive military planning to address evolving global security dynamics influenced by extreme weather events.

One of the more significant areas of underestimation is the potential for simultaneous, compounding events such as a synchronous failure of multiple global breadbaskets due to extreme weather[110]. This could trigger widespread food insecurity, social unrest, and migration pressures, straining military resources and further complicating existing geopolitical tensions. Soaring food prices due to extreme weather events that resulted in droughts and harvest losses in major wheat-producing regions such as China and Eastern Europe are believed to be precipitating conditions for social unrest that culminated in the series of protests and uprisings known as the Arab Spring[111,112].

The timescale of climate impacts is another area where current thinking falls short. While some effects are gradual, others can manifest rapidly, particularly when tipping points are crossed. The defence sector's long-term planning horizons, while necessary for major acquisitions and infrastructure projects, may inadvertently lead to a false sense of having time to adapt gradually to climate change. Furthermore, the MOD's current approach often treats climate change as a distinct, somewhat isolated issue. However, its impacts are likely to intersect with and exacerbate other security challenges in complex ways[113].

110 Gaupp, F., Hall, J., Hochrainer-Stigler, S., & Dadson, S. (2020). Changing risks of simultaneous global breadbasket failure. Nature Climate Change, 10(1), 54-57.

111 Soffiantini, G. (2020). Food insecurity and political instability during the Arab Spring. Global Food Security, 26, 100400.

112 Sternberg, T. (2012). Chinese drought, bread and the Arab Spring. *Applied Geography*, 34, 519-524.

113 Mach, K. J., Kraan, C. M., Adger, W. N., Buhaug, H., Burke, M., Fearon, J. D., ... & von Uexkull, N. (2019). Climate as a risk factor for armed conflict. Nature, 571(7764), 193-197.

For instance, climate-induced resource scarcity could fuel conflicts in strategically important regions, creating new demands on UK military resources and capabilities. An illustrative example are the unprecedented heat waves in the Sahel region which have intensified existing challenges, exacerbating intercommunal tensions, heightening competition for scarce resources, and potentially fuelling radicalisation[114,115,116].

Climate change-induced shocks are increasingly complicating global security dynamics. The potential for climate change to reshape geopolitics can no longer be considered a peripheral factor but must be integral when devising overall strategic defence and security policy.

The frequency of climate-related military deployments, which has surged dramatically, illustrates this. In 2024 armed forces from 62 nations, including major powers, including the US, China and Germany, were mobilised to address climate-induced crises.[117] This period saw 250 deployments for climate-related military operations.[118] Climate change also has tangible impacts on human security and prosperity, beyond those of purely national defence and security. For example, recent studies suggest that extreme weather events may have contributed up to one-third of the rises in food prices that occurred in the UK between 2022 and 2023.[119] The impacts of this had a consequential impact on the outcome of the 2024 UK elections.

The rapid acceleration of climate impacts presents adaptation challenges for the defence sector and leads to an ever-increasing gap between the evolving threat landscape and current preparedness levels. This does not even start to consider the increasing risk of Earth system tipping points [120] such as major ice sheet collapse or ocean circulation shutdown. Such events would abruptly alter the face of the planet irrevocably with profound implications for global security[121]. The potential for these tipping points to cascade, creating compound effects that amplify and accelerate climate impacts, represents a critical blind spot in current defence planning and risk assessment frameworks[122].

Necessary Changes to Defence Strategy: A Strategic Imperative

Given the underestimation of climate impacts, a fundamental reassessment of UK defence strategy is urgently needed. This should strive for a comprehensive view of the threats to UK security from the climate crisis, supplementing and filling the gap between the current Climate Change Risk Assessment[123] and National Security Risk Assessment processes.

114 www.sipri.org/publications/2019/sipri-policy-briefs/climate-change-peacebuilding-and-sustaining-peace

115 Kazeem, O. S. (2024). Climate change and violent conflict in the Sahel and Lake Chad Basin. *Journal of Contemporary International Relations and Diplomacy*, 5(1), 74-85.

116 Akinyetun, T. S., Fatai-Abatan, A., & Ogunbodede, N. (2024). Heated Environment, Armed People: Between "Climate Change Conflict" and "Fragility Conflict" in the Sahel. *Journal of Asian and African Studies*, 00219096241285108.

117 councilonstrategicrisks.org/ccs/mirch

118 councilonstrategicrisks.org/ccs/mirch

119 eciu.net/analysis/reports/2023/climate-fossil-fuels-and-uk-food-prices-2023

120 Armstrong McKay, D. I., Staal, A., Abrams, J. F., Winkelmann, R., Sakschewski, B., Loriani, S., ... & Lenton, T. M. (2022). Exceeding 1.5 C global warming could trigger multiple climate tipping points. Science, 377(6611), eabn7950.

121 Lenton, T. M., Rockström, J., Gaffney, O., Rahmstorf, S., Richardson, K., Steffen, W., & Schellnhuber, H. J. (2019). Climate tipping points—too risky to bet against. Nature, 575(7784), 592-595.

122 Wunderling, N., Donges, J. F., Kurths, J., & Winkelmann, R. (2021). Interacting tipping elements increase risk of climate domino effects under global warming. Earth System Dynamics, 12(2), 601-619.

123 Department for Environment, Food and Rural Affairs. (2022). UK Climate Change Risk Assessment 2022. GOV.UK. www.gov.uk/government/publications/uk-climate-change-risk-assessment-2022

In addition to the initiation of the national security risk assessment of climate change, to address these urgent challenges and strategic imperatives the following changes to defence strategy are necessary:

1. Integrate climate considerations beyond adaptation, reassessing force structures, equipment needs and operational doctrines to address fundamental changes in the strategic context.
2. Include nonlinear (tipping points), compounding and cascading risks on the UK's national risk register.
3. Improve climate knowledge throughout the national security workforce by comprehensive training and education, using climate scenarios in various exercises for planning.
4. Improve interdepartmental coordination on climate security issues, with other government departments regarding climate policy, conflict prevention, energy security and supply chain resilience.
5. The MOD should aim to be the world leader in climate security, leading climate-resilient military operations within NATO and other international fora.
6. Develop planning processes in which strategic assumptions are periodically reassessed to respond to rapidly changing climate-security dynamics.
7. Increase involvement in broader societal resilience building efforts to address shared vulnerabilities by collaborating with local authorities, critical infrastructure operators, and emergency services.

A coordinated MOD strategy that includes adaptation investments, enhancing institutional resilience, and a comprehensive risk evaluation is necessary to robustly address climate change related issues. Failure to prioritise climate resilience may lead to operational disruptions, widening capacity gaps, and monetary losses. It will cost billions of pounds to climate-proof military infrastructure, but the cost of inaction will be far greater.[124]

124 Ackerman, J. R., & Andrews, E. (2022). "The Security Threat That Binds Us: The Unraveling of Ecological and Natural Security and What the United States Can Do About It." The Wilson Center.

Do we fully understand the security threat posed by online extremism and self radicalisation?

Dr Lewys Brace

At 13:28NZDT on 15th March 2019, a message appeared on the anonymous image board *8chan/pol* stating, "Well lads, it's time to stop shitposting and make a real life effort post. I will carry out and *(sic)* attack against the invaders, and will even live stream the attack via facebook". The post included links to a manifesto document and a Facebook live stream. Moments later, the post's author, Brenton Tarrant, began an attack on two separate mosques in Christchurch, New Zealand, resulting in the deaths of 51 people.

Tarrant was clearly motivated by right-wing extremist (RWE) ideology, as demonstrated by his use of racist rhetoric and discussions of 'the great replacement' theory and other RWE tropes. Crucially, the subsequent inquiry into his attack found Tarrant to have been an active participant in an online extremist ecosystem of content[125]. His activity was inspired by discussions on *8chan/pol*[126] (NO2) and other similar platforms. He used *8chan/pol* to advertise his attack and present his justifications, with his manifesto and cultural references during the livestream being designed to appeal specifically to the online audience of *8chan/pol*. He has subsequently become known as a "hero" or "saint" on these online spaces, and his actions have inspired others to carry out attacks using a similar modus operandi[127].

How Domestic Online Extremism is changing

The Christchurch case highlights two aspects of domestic online extremism that have become prominent over the last decade. First, Tarrant is an example of what UK authorities refer to as 'self-initiated terrorists' (SITs). These are individuals who do not have any personal links, direction, or material support from a terrorist/extremist organisation or group, but who are influenced by ideological material they have engaged with.[128] Second, it supports empirical evidence that has shown how online spaces, such as *8chan/pol*, are not merely places of 'harmless' and 'edgy' discussions with 'dark humour', but are instead radicalising milieux in their own right due to their subcultural dynamics.[129]

Furthermore, advancements in communication technologies have ensured these online extremist spaces do not exist in isolation, but are instead part of a network of interacting online spaces; often conceptualised as an "ecosystem".[130] These online spaces are often characterised by identity-based subcultures that are defined by notions of in-group and out-group(s) identity, with intergroup competition being presented as a crisis-solution

125 Royal Commission of Enquiry, 'Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain on 15 March 2019', 2020, christchurchattack.royalcommission.nz

126 8chan is one iteration of a family of anonymous imageboard sites (forums that are characterised by lack of usernames and large use of images in posts), with other iterations including 4chan, 9chan, Neinchan, etc. Each iteration has a series of thematic boards, with the /pol (short for "politically incorrect") boards being known for hosting racist, misogynistic, and homophobic content.

127 Stephane J. Baele, Lewys Brace, and Travis G. Coan, 'The "Tarrant Effect": What Impact Did Far-Right Attacks Have on the *8chan* Forum?', *Behavioral Sciences of Terrorism and Political Aggression*, 22 December 2020, 1–23, doi.org/10.1080/19434472.2020.1862274

128 See National Counter-Terrorism Security Office. 'Self-Initiated Terrorists (S-ITs)', 2021. www.protectuk.police.uk/threat-risk/threat-analysis/self-initiated-terrorists-s-its

129 Baele, Brace, and Coan, 'The "Tarrant Effect"'; Lewys Brace, Investigating the Far-Right Online: Using Text Data to Understand Online Subcultures ([object Object], 2022), doi.org/10.5258/NCRM/NCRM.00004548

130 Stephane J. Baele, Lewys Brace, and Travis G. Coan, 'Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda', Studies in Conflict & Terrorism, 30 December 2020, 1–21, doi.org/10.1080/1057610X.2020.1862895; Jade Hutchinson et al., 'Violent Extremist & REMVE Online Ecosystems: Ecological Characteristics for Future Research & Conceptualization' (RESOLVE Network, 25 August 2022), doi.org/10.37805/remve2022.5

narrative.[131] This is the kind of ecosystem in which Tarrant was a participant. They are likely to be part of the reason, as recent research has demonstrated, that acts of extremist violence, which take place without any online influence, are becoming increasingly rare at the same time as there is an increase in SIT cases in Europe and the USA.[132]

Changing radicalisation patterns

These SITs cases have been hard to detect due to their nature, and there is now evidence that this phenomenon is evolving in ways that will present further issues. Namely, technological affordances are driving an increase in younger individuals forming their own bespoke ideology that aligns with their own personal experiences and grievances, and which draws upon ideas from several more established ideologies and extreme worldviews. Evidence for this comes from four data-driven insights.

Recent years have seen an increasing number of young people engaging with extremist content.

Taking the UK as an example, in the year ending September 2022, there was a substantial increase in the number of individuals aged 10-20 being arrested for terrorism offences; the first time this age group had outnumbered the 21-29 age group.[133]

At the same time, there has been a marked increase in the number of individuals engaging with ideologies that are known as 'convergent violent extremist ideologies',[134] 'salad bar' ideologies[135] or 'Mixed, Unclear, or Unstable' (MUU) ideologies; the last term being the UK's official designation. These ideologies are defined as those that combine components of different ideologies together (mixed), evolve and change quickly as their components become more or less favoured by the individual (unstable), or are incoherent (unclear).(WY3) The emerging academic research refers to this phenomenon as 'ideological cross-pollination' and 'fringe fluidity',[136] with some arguing that this should be viewed as a distinct radicalisation pathway in its own right.[137] Again, taking the UK as an example, this type of ideology is not only becoming a prominent part of the domestic extremist landscape, but seems to be a radicalisation pathway that is largely dominated by young people.[138]

131 J M Berger, Extremism (The MIT Press, 2018), doi.org/10.7551/mitpress/11688.001.0001

132 Georgia F. Hollewell and Nicholas Longpré, 'Radicalization in the Social Media Era: Understanding the Relationship between Self-Radicalization and the Internet', International Journal of Offender Therapy and Comparative Criminology 66, no. 8 (June 2022): 896–913, doi.org/10.1177/0306624X211028771; Jonathan Kenyon, Jens Binder, and Christopher Baker-Beall, 'Understanding the Role of the Internet in the Process of Radicalisation: An Analysis of Convicted Extremists in England and Wales', Studies in Conflict & Terrorism, 24 April 2022, 1–25, doi.org/10.1080/1057610X.2022.2065902; Daniele Valentini, Anna Maria Lorusso, and Achim Stephan, 'Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization', Frontiers in Psychology 11 (24 March 2020): 524, doi.org/10.3389/fpsyg.2020.00524

133 See: Home Office. 'Operation of Police Powers under the Terrorism Act 2000 and Subsequent Legislation: Arrests, Outcomes, and Stop and Search, Great Britain, Quarterly Update to September 2022', 2022.

134 US Department of Homeland Security, 'National Terrorism Advisory System Bulleting: February 7, 2022 - 2:00 PM ET', 2022, www.dhs.gov/sites/default/files/ntas/alerts/22_0207_ntas-bulletin.pdf

135 Matthew Alcoke, 'The Evolving and Persistent Terrorism Threat to the Homeland. Https://Www.Washingtoninstitute.Org/Policy-Analysis/Evolving-and-Persistent-Terrorism-Threat-Homeland', www.washingtoninstitute.org/policy-analysis/evolving-and-persistent-terrorism-threat-homeland

136 M Criezis, 'Intersections of Extremisms: White Nationalist/Salafi-Jihadi Propaganda Overlaps and Essentialist Narratives about Muslims', Journal of Education in Muslim Societies 2, no. 1 (2020), https://muse.jhu.edu/article/811620/pdf; G Gill, 'Fascist Cross-Pollination of Australian Conspiracist Telegram Channels', First Monday 26, no. 12 (2021), https://doi.org/10.5210/fm.v26i12.11830; Ariel Koch, 'The ONA Network and the Transnationalization of Neo-Nazi-Satanism', Studies in Conflict & Terrorism, 12 January 2022, 1–28, doi.org/10.1080/1057610X.2021.2024944

137 Daveed Gartenstein-Ross et al., 'Composite Violent Extremism: Conceptualizing Attackers Who Increasingly Challenge Traditional Categories of Terrorism', Studies in Conflict & Terrorism, 29 March 2023, 1–27, https://doi.org/10.1080/1057610X.2023.2194133; Daveed Gartenstein-Ross and Madeleine Blackman, 'Fluidity of the Fringes: Prior Extremist Involvement as a Radicalization Pathway', Studies in Conflict & Terrorism 45, no. 7 (3 July 2022): 555–78, https://doi.org/10.1080/1057610X.2018.1531545.

138 Lewys Brace, Stephane J. Baele, and Debbie Ging, 'Where Do 'mixed, Unclear, and Unstable' Ideologies Come from? A Data-Driven Answer Centred on the Incelosphere', Journal of Policing, Intelligence and Counter Terrorism 19, no. 2 (2 April 2024): 103–24, doi.org/10.1080/18335330.2023.2226667

Online behaviours are changing; all age groups are spending more time online, with this increase being most significant amongst teenagers.[139] Research now argues in favour of not viewing online and offline behaviours and personas as distinct, but instead, understanding that individuals are increasingly integrating their online and offline experiences when forming their personality and behaviours.[140]

Advancements in communication technologies continue to change how individuals engage with online content by offering various, and sometimes novel, affordances; i.e. the ability to share content, comment on the posts of others, and tagging other users. Online extremist communities have demonstrated that they are, both consciously and sub-consciously, eager adopters of such affordances; with studies attributing many of the recent trends seen in online extremism to the use of such online affordances (NO4).[141] The impact of such affordances cannot be understated, especially given recent advancements in generative AI. Given the history and past behaviours of such online communities as those that inhabit sites such as *8chan/pol*, it is likely that they could make use of this technology in 5 distinct ways - propaganda generation; blackmailing/ harassment; platform boosting, polluting the information environment and developing misperception-inducing content.[142]

The Internet Remains the Breeding Ground

It is hypothesised that these factors are all inter-related, with the increasing number of MUU cases being driven by expanding ecosystems of extremist content. This results in certain online spaces acting as gateways to other online spaces that host more radical content, and which are more integrated into their respective ecosystems. Crucially, such gateway spaces are sometimes not extremist in nature themselves but have some users who post links to extremist online spaces and content. This use of the linking affordance appears to sometimes be strategic to establish links between online spaces, while other times, it appears to be subconscious with individuals sharing content "of interest to the discussion". Regardless of motives, over time this behaviour results in both certain spaces acting as gateways to extremist content and contributes to the mainstreaming of certain extremist ideas that have originated in extremist online spaces.

It is believed that young people are particularly vulnerable to the effects of this linking behaviour, even if they are not actively seeking out such content. This is because their young age means they are likely to be undergoing a process of socialisation, resulting in some of these ideas providing "answers" to their personal insecurities due to their identity-based nature; this has been demonstrated with more established ideologies, such as the incel worldview.[143] While substantial empirical evidence of this phenomenon is yet to emerge, some early studies do support it. For example, a data-driven approach has been used to show that the MUU phenomenon was being driven by users making use of linking between different online spaces, sometimes, (but not always) strategically, and that this technological affordance allows individuals to be easily exposed to different notions from various ideologies and online subcultures, sometimes from other extremist ecosystems.

139 Monica Anderson and Jingjing Jiang, 'Teens, Social Media & Technology 2018', Pew Research Center, 2018, www.pewresearch.org/internet/wp-content/uploads/sites/9/2018/05/PI_2018.05.31_TeensTech_FINAL.pdf; Ofcom, 'Online Nation - 2021 Report', 2021, 185, www.ofcom.org.uk/__data/assets/pdf_file/0013/220414/online-nation-2021-report.pdf

140 Primavera Fisogni, 'Cyber Terrorism and Self-Radicalization - Emergent Phenomena of Onlife Age: An Essay Through the General System Theory', International Journal of Cyber Warfare and Terrorism 9, no. 3 (2019); Valentini, Lorusso, and Stephan, 'Onlife Extremism'.

141 Brace, Baele, and Ging, 'Where Do 'mixed, Unclear, and Unstable' Ideologies Come From?'; A Corbeil and R Rohozinski, 'Managing Risk: Terrorism, Violent Extremism, and Anti-Democratic Tendencies in the Digital Space', in The Oxford Handbook of Cyber Security, ed. P Cornish (Oxford: Oxford University Press, 2021), 163–72; S Peeters and T Willaert, 'Telegram and Digital Methods: Mapping Networked Conspiracy Theories through Platform Affordances', M/C Journal 25, no. 1 (2022), https://doi.org/10.5204/mcj.2878; Xinyi Zhang and Mark Davis, 'E-Extremism: A Conceptual Framework for Studying the Online Far Right', New Media & Society, 7 June 2022, 146144482210983, https://doi.org/10.1177/14614448221098360

142 Stephane J Baele and Lewys Brace, 'AI Extremism: Technologies, Tactics, Actors' (VoxPol, 2024), voxpol.eu/new-vox-pol-report-ai-extremism-technologies-tactics-actors

143 Lewys Brace, 'Incels and the Incelosphere: An Overview of Current Research and Understanding' (Centre for Research and Evidence on Security Threat, 2023), crestresearch.ac.uk/resources/incel-and-the-incelosphere-an-overview-of-current-research-and-understanding

A Way Forward

This emergent phenomenon is likely to increase in frequency in future years given technological advancements and subsequent changes to our behaviours. However, more empirical and data-driven work is required to increase our understanding of both this phenomenon itself and to allow for the development of effective detection and deradicalisation approaches.

A first step would involve understanding how these ecosystems expand, under what circumstances a significant amount of links are made between an online space hosting extremist content and other online spaces, which ideas gain traction, and whether this is related to real-world, offline, events.

The University of Exeter has a large number of researchers with both substantive expertise in such areas and research methods expertise through the existence of the Centre for Computational Social Science and Institute for Data Science and Artificial Intelligence.

This dual expertise allows these researchers to provide novel and actionable insights into online extremism, terrorism, and other homeland security-related issues.

A second step would be to beef up existing legislation. In particular, this should include the Online Safety Act, plus the National Cyber Security Agency and other government agencies, forming a more holistic approach to combatting this growing phenomenon. This top-down approach should also be accompanied by a bottom-up approach that involves community-based measures, such as including lessons on how to spot mis/disinformation and extremist or radical content as part of the national curriculum.

Lastly, an emphasis on tackling the root causes of attraction towards domestic online extremism, which is a whole government and societal issue.

University *of* Exeter

Exeter Defence,
Security and Resilience

2024HASS040