THE BRITISH ARMY REVIEW

AUTUMN 2023 / ISSUE #185

FORCE PROJECTION: HOW WE WILL FIGHT IN THE FUTURE

THE JOURNAL OF BRITISH MILITARY THOUGHT

ARMY

THE
BRITISH ARMY
REVIEW
ISSUE #185 / AUTUMN 2023

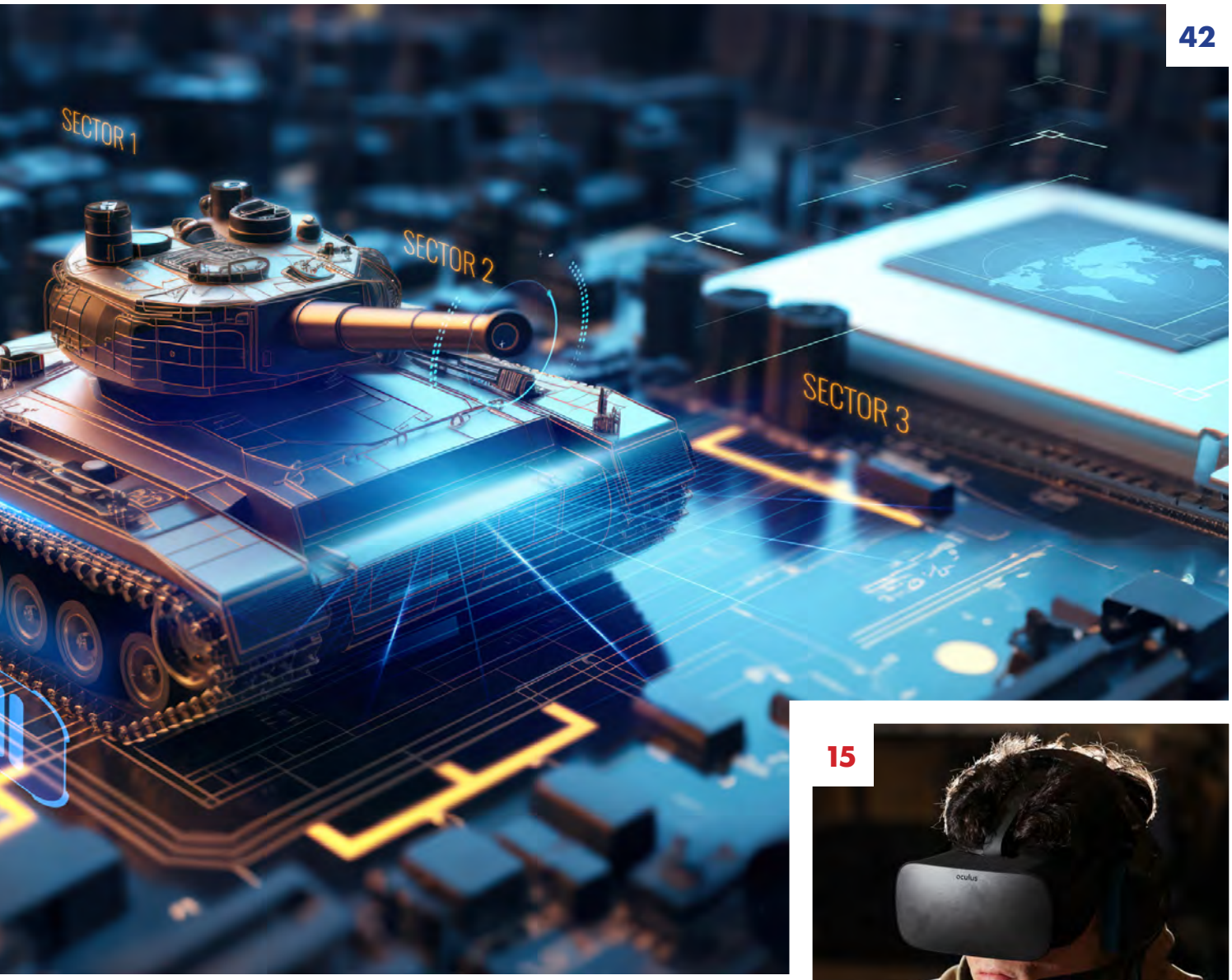
The British Army Review, Robertson House, Royal Military Academy Sandhurst, Camberley GU15 4NP

Email: editorBAR@chacr.org.uk

CHACR

IN THIS ISSUE...

THEMED ESSAYS: ARMY FUTURES



42

15

Courtesy of Soldier Magazine © Crown copyright

GENERAL ARTICLES

REVIEWS

FOCUS ON THE 'NOW, NEXT' AND FUTURE' IS NECESSARY TO 'REMAIN WORLD BEATERS'

THIS edition of *The British Army Review*, the third of 2023, follows on from the previous two issues, the first of which (with its foreword by the Chief of the General Staff) focussed on immediate mobilisation, and the second of which (with its foreword by Commander Field Army) considered how we will 'fight tonight' and fight over the next few years. The logic flow of the year, therefore, is completed in this publication, with the lead articles examining what Project Wavell and Future Soldier are telling us about the way that we can expect to fight in the coming decades.

The three editions together take the reader from the readiness of the Army, now, to address all of those challenges that may be thrown at it, through the expected proximate challenges and out into the realms of force development to deal with expected (and unexpected) future challenges. In the second part of this publication you can find the usual spread of articles of general professional interest, from an interview with a senior representative of the IT Army of Ukraine, through thoughts on 'Cyber Peacekeeping', to cautionary operational-level tales from Iraq, and then, in its final third, the by-now traditional insight into up-coming or recently published Army and Defence concepts and doctrine, along with defence-related book, podcast and other media reviews.

Importantly, work on concepts for the future, even when those concepts are turned into force development, operating instructions or doctrine, are only effective if the superstructure of the Army is properly trained and equipped and the substructure is firm, stable and enduring. It is worth pointing out, therefore, that the 'Futures' work that is explored in the opening section of this issue of *The British Army Review* is underpinned by work on the two key areas of 'Agile Procurement' and 'The Institutional Foundation' of the Army, which is being conducted in Army HQ, the Field Army and Home Command (supported in all cases by the CHACR). In the first case, the future Army will depend very heavily on our procurement and acquisition process being able to keep up with the ever-increasing tempo of technological change: gone are the days when military kit can afford to take many years to procure and then expect to last for decades and hope to remain useful in the face of the enemy.

"Work on concepts for the future, even when those concepts are turned into force development, operating instructions or doctrine, are only effective if the superstructure of the Army is properly trained and equipped and the substructure is firm, stable and enduring."

At the same time, and in the second case, such evolution can only hope to change the superstructure of the Army (its order of battle and equipment tables, for example) if it is built on a firm and lasting foundation – which sits at the heart of Home Command's 'Institutional Foundation' work. The French Army's equivalent of Home Command has a pithy but meaningful strap line: être et durer (to be and to endure) – Home Command will continue to make sure, as we evolve the Army, at pace, to keep up with an ever-changing threat kaleidoscope alongside an increasingly rapidly-evolving world of technology, that it retains those foundational aspects that make sure that the men and women who serve in it are enabled to remain world beaters.

This edition of *The British Army Review*, therefore, covers much ground and, when taken in conjunction with this year's two preceding issues, provides the professional reader with profound insight into the 'now, next and future' of the British Army. I commend it to you. **– Lieutenant General Sharon Nesmith, Deputy Chief of the General Staff**

FROM THE EDITOR

My professional 'brush' with the British Army has been sustained and close enough to put a serious dent in the once cast-iron convictions I held as a fledgling journalist about the power of the written word.

For a civilian ever green to the stark realities of combat, the pen certainly does not feel mightier than the sword when you find yourself in range of enemy mortar fire, cowering in a Scud trench or on hearing your host unit being ordered to 'stand to'.

Throughout history, wars have served to significantly sharpen the edge of the metaphorical sword, with advances in technology making its blows ever more accurate and deadly. In contrast, it can be argued that the pen's ability to affect social, cultural or political change has been blunted by the advent of social media and citizen journalism. Accuracy and balance all too frequently find themselves as casualties of immediacy, the prioritisation of clicks over credibility and deliberate attempts to misinform.

There is, however, still some truth to be found in the metonymic adage – as I hope the pages of this *British Army Review* testify. Take, for example, how words – albeit constrained to 280 characters in the case of the part played by the app formerly known as Twitter – have helped Ukraine to raise a formidable international force. As detailed in our interview with a senior member of the IT Army of Ukraine, a very modern call-to-arms has seen more than 230,000 anonymous volunteers mobilised in support of the group's battle for cyber supremacy with Russia.

Closer to home, language is a key component of the arsenal being deployed by Army Futures as it scans the horizon and attempts to build a picture of what is likely to lie beyond the line-of-sight for land forces. Articulating the conceptual toil and supporting analysis that continues to be undertaken to refine the Service and drive change into the 2030s is a challenge that must be conquered if the Land Operating Concept – *A New Way of Winning* – is to prove the firm foundation on which the future of the Army is built. Convincing internal and external stakeholders of this new direction's validity will, to quote Major General James Bowder, increase "the consistency and coherence of army force development" and improve "the quality of the capability and resource conversation with the broader defence community, across government and internationally".

The words in the articles that follow are grist to this mill and the professional thinking they are intended to provoke will assist in oiling the Army's blade for tomorrow's battles. – **Andrew Simms**

THE LAND OPERATING CONCEPT – A NEW WAY OF WINNING

AUTHOR

Major General James Bowder is Director Army Futures, responsible for setting the aiming point of the British Army and driving change. He previously commanded 1st Intelligence, Surveillance and Reconnaissance Brigade and the 6th (United Kingdom) Division.

IN the two most recent editions of *The British Army Review*, the Chief of the General Staff re-emphasised the need for the British Army to mobilise and Commander Field Army underlined the importance of being ready to fight tonight. In addition, we also need to plan and prepare for the future so that we are ready to fight and win wars tomorrow. This requires a conceptually driven, threat aware approach to force development. One that starts by defining a way of winning fit for the 21st century, and that slaves its future capability and force structural judgments to bringing this new approach into being. This article will briefly introduce the Land Operating Concept – *A New Way of Winning* and place it in context.

Armies need firm conceptual foundations. An externally validated land operating concept not only increases the consistency and coherence of army force development through time, but also improves the quality of the capability and resource conversation with the broader defence community, across government and internationally. As such, a land operating concept is akin to source code: a vital building block that drives everything else.

The British Army's new Land Operating Concept – *A New Way of Winning* is the first, and foundational, deliverable of Project Wavell, the Army's exercise to refine its aiming mark and drive change into the 2030s. The concept builds on *Future Soldier* and Field Army's *How We Fight 2026*. Moreover, it aligns with Defence's *Future Operating Concept* and is driven both by NATO's strategic concept for the deterrence and

defence of the Euro-Atlantic area, and its long-term conceptual vision detailed in the NATO Warfighting Capstone Concept.

The Land Operating Concept has taken more than 18 months to develop. As can be seen in the articles that follow, it draws upon a broad evidence base and has been rigorously tested. We, in Army Futures, are extremely grateful for the energetic engagement of the Field Army, the Defence Science and Technology Laboratory, broader defence, academia, industry and overseas partners in the construction of the document. It is a great deal better as a result.[1] Turning to the headlines of the new approach espoused by the Land Operating Concept, I will first set out how we see the future operating context, before explaining how we will gain advantage.

THE CHALLENGE

Competing states will present conventional and unconventional military threats to the UK and her interests during the next decade. In parallel, instability driven by violent extremists, climate change, evolving demographics and the malign activity of hostile states will play-out beyond our near abroad. This will necessitate the British Army offering value in several different directions simultaneously.

Demands upon the Army will increase at home due to the growing physical and virtual reach of state competitors, and the continuing challenge presented by violent extremists, extreme weather and pandemics.

Climate change and the path to net zero will shape the land force, presenting both opportunities and challenges to overcome. Furthermore, so-called 'black swan' events will occur and place a premium on the Army's agility, flexibility, and adaptability.

Future land battle will be characterised by continuity and change. First, continuity:

"The prevalence of autonomous platforms will continue to increase. In part through the introduction of ever-more ambitious uncrewed ground vehicles, but more importantly through the continued commoditisation of drones, which will force soldiers to always think in three dimensions."

- During the next decade land battle will remain violent and visceral, a trial by fire where novel technologies increase lethality and cost. Here the moral component and will to win will be as important as ever, placing a particular onus on combat cohesion and the resilience of our soldiers.

- Logistics continues to sit on the critical path. Clever new precision missiles will be for nothing unless we can get them to their launchers through highly contested lines of communication.

- And of course, land battle will continue to be a contest of systems where the quality of combined arms integration is a key determinant of success and competence in this integration comes from practise in demanding training.

That said, alongside this continuity we predict that the character of the land battlefield will evolve significantly during the next decade driven by the following four themes:

- Precision munitions, coupled with ever more advanced sensor technology, have brought about something of a find and fires revolution during the past decade.[2] This shows little sign of abating – just the opposite in fact – increasing reach and jeopardy on a more transparent and treacherous battlefield in the next ten years.[3]

- The prevalence of autonomous platforms will continue to increase. In part through the introduction of ever-more ambitious uncrewed ground vehicles, but more importantly through the continued commoditisation of drones, which will force soldiers to always think in three dimensions. Moreover, autonomous artificial intelligence-powered target acquisition and decision support capabilities will enable offensive and defensive operations at machine speed.

- Both these developments will markedly increase the data, software and digital dependence of land forces. As kill-chains become ever more integrated and autonomous so their attack surface will increase in the hyper-contested electromagnetic spectrum and cyberspace.[4]

- Finally, combat will play out in something of a goldfish bowl under the full glare of the public gaze, given the prevalence of mobile technology and new media, complicating surprise, deception and the maintenance of consent.

Whilst technology will continue to drive tactics, it will not wholly define competitiveness. Training, the quality of personnel and the will to fight will continue to sit on the critical path. Indeed, the spirit, resilience and ingenuity of soldiers will matter more than 'stuff'. Multi-domain dependencies, vulnerabilities and opportunities will increase, whilst alliances and bi-lateral partnerships will continue to matter disproportionality. So too will strategic affordability.

Taken together the crux of the Army's

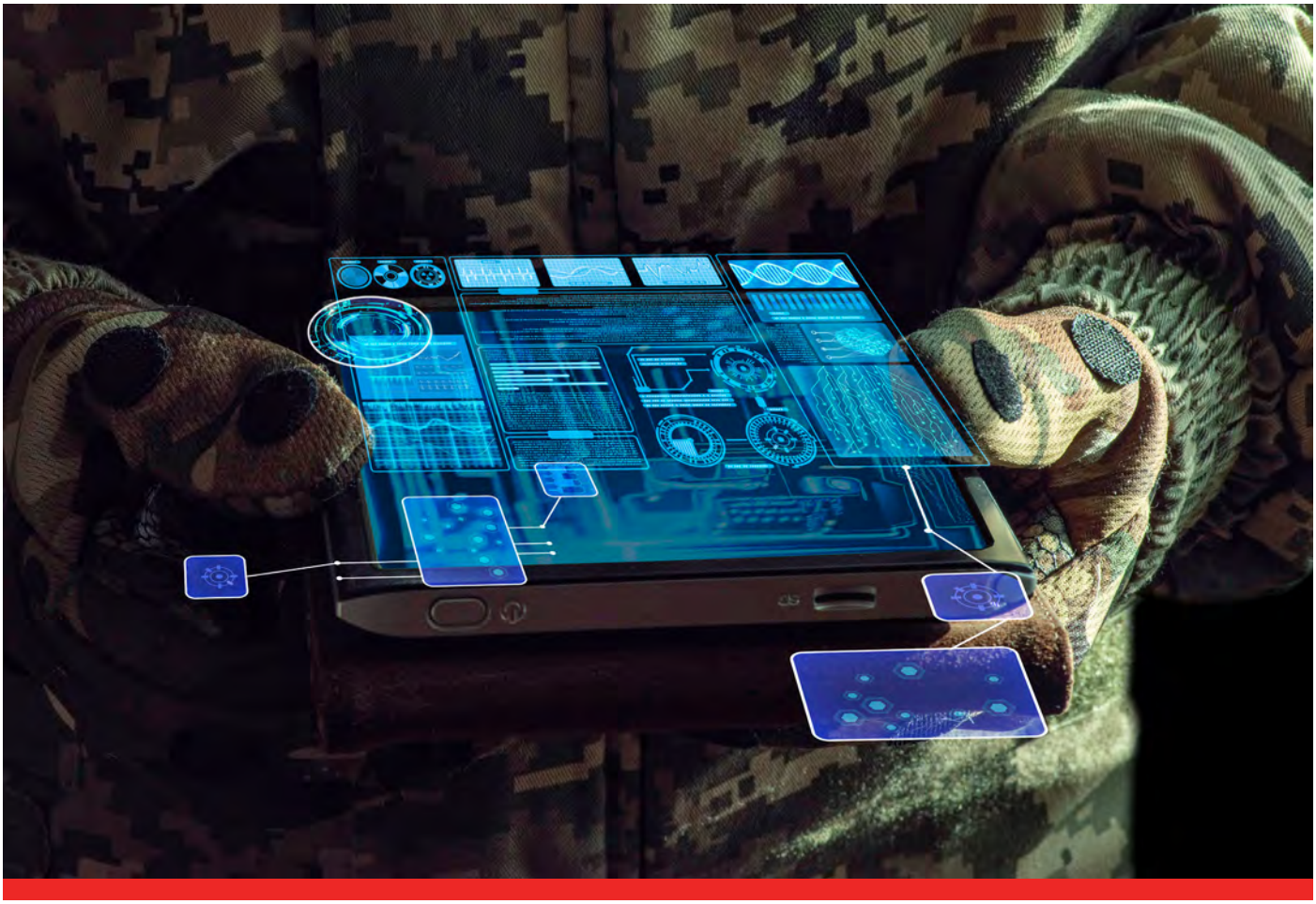
---

[1] *As General Donn Starry, the architect of AirLand Battle, wrote: "Changes must be subjected to trials, their relevance convincingly demonstrated to a wide audience by experiment and experience, and necessary modifications made as a result of trial outcomes." Military Review, March 1983.*

[2] *Jack Watling's The Future of Fires, RUSI Occasional Paper from November 2019 is a good start point to explore the trend.*

[3] *The recent article by Shashank Joshi in the Economist (3rd July 2023) on Lessons from Ukraine echoes many of the points made within the Land Operating Concept.*

[4] *Kill chain: an orderly chain of interdependent links in the process of striking a target, consisting of four components: control equipment, sensor equipment, strike equipment (weapon and platform), and evaluator equipment, with the operations divided into six components in six phases: find, fix, track, target, engage, and assess, or F2T2EA.*



"Land forces must confront the reality that competence in the electromagnetic spectrum and cyberspace will be a key determinant of success on a future battlefield, given that both will be congested and energetically contested."

challenge over the next decade is being able to win land battles in Europe – thereby contributing to NATO's deterrence effort – whilst also meeting broader outputs at home and outside Europe. And to do so in a manner that is strategically affordable and transparently productive.

THE ARMY'S RESPONSE – A NEW WAY OF WINNING

To achieve advantage within this context we will need to adopt a new way of winning. This will see us:

Redefine readiness. Speed matters. To help NATO deter an opportunistic enemy land-grab – and resist it if it materialises – the UK's land forces will need to be nimble, front-footed and expeditionary. Ready quickly, deployable at pace, sustainable and survivable, the UK's first fighting echelon in the land domain must be sufficiently agile, resilient, and reliable to provide catalytic value to Supreme Allied Commander Europe as a crisis unfolds. This heightened responsiveness will improve the credibility and effect of NATO's deterrence in the land domain.

Campaign relentlessly. Whilst armies exist to fight and win battles, the forces optimised to do this should also make a significant broader contribution, given the complex and manifold security demands of the next decade. As part of His Majesty's Government's international recce screen, the land force must help Britain foster relationships to secure access and influence in Europe, Africa, the Middle East and the Indo-Pacific. By applying an entrepreneurial approach to opportunity and advantage, land forces can act as an instrument of foreign policy, and a tool leverageable in leader-to-leader engagement. Similarly, the land contribution to defence exports must be front-footed and activist.

Enable success cross-domain. During the next decade, each domain will become more contested and dangerous. Intelligence, surveillance and reconnaissance and fires operated from the land domain can increase the freedom of action of UK or alliance forces in the maritime, air, space and cyber electromagnetic domains. UK land forces will never operate in a vacuum. They will have wide-ranging dependencies on the other domains, their partners and allies. But the future will see UK land forces shifting the balance from being a net demander from this multi-domain enterprise to a net contributor. To effect this rebalance, the Army will need to be imaginative and extrovert in how it sets the conditions for the broader Joint Force's success.

Adapt at pace. Given the agility of our adversaries and the opportunities afforded by disruptive technology, land forces will need to be able to adapt at pace, both in and out of contact. Increasingly, competitiveness will be 'software-defined' with land forces deriving greater value from the systems hung on their battlefield platforms, than the platforms themselves in a traditional sense. Therefore, the harvest, analysis and distribution of 'mission data' in contact, and the rapid construction of software solutions in response, will be critical for tactical adaptation. As such an approach evolves, the demands on interoperability will become even more acute; not only cross-domain and multinationally, but internally and with industry. The procurement of Army platforms that seamlessly enable data exchange across all systems, all domains and within the supply chain will become a fundamental requirement.

Fight and operate differently. As a priority, land forces urgently need to come to terms with the implications of the evolving character of conflict outlined in the previous section. That is, one which will be less linear, often defensive in character, where towns will invariably be the principal prize – alongside access to resources – and where manoeuvre in open, rural terrain takes place amid particular jeopardy. It will be difficult to survive, to prosper offensively and to win cheaply either as the attacker or the defender. In response, the British Army will place particular emphasis on five imperatives during the next decade:

- **Fight by recce-strike at every level.** Legacy tactical schema that instinctively bias offensive rural manoeuvre culminating in a decisive act in the close battle fail to acknowledge the opportunity presented by contemporary and future stand-off find and fires capabilities, as well as the attendant challenge of survival. New tactical approaches are required that reflect this evolving reality, as well as the disruptive potential of robotics, autonomy and artificial intelligence. Specifically: the adoption of a recce-strike methodology from battlegroup to corps levels, maximising stand-off find and lethality, drawing – where available – upon assets from each domain.

- **Treat survival as a deliberate operation.** Surviving on a 21st century battlefield is a challenge. Dispersal is only part of the answer. Land forces will also need to leverage helpful terrain such as towns, which make them harder to acquire as targets. A more active and deliberate approach to suppressing the enemy's find and fires complex will also be required. This counter-kill-chain activity will need to achieve a relentless tempo of counter-intelligence, surveillance and reconnaissance, counter-command and control and counter-fires operations, throughout the battle. Similarly, multi-spectral concealment and deception will be critical to success. Deft signature management and spoofing will significantly increase survivability.

- **Manoeuvre aggressively in the electromagnetic spectrum and in cyberspace.** Land forces must confront the reality that competence in the electromagnetic spectrum and cyberspace will be a key determinant of success on a future battlefield, given that both will be congested and energetically contested. Outmanoeuvring, outpacing and outmatching an opponent here will invariably lead to tactical advantage. It will be an important front line during conflict, and one where we will need to set the conditions for success out of contact. In part this will necessitate the hardening of networks and building resilience and redundancy into kill-chains. Finally, we must train to 'fight through' and, should it be necessary, 'fight without' periods of overmatch in the electromagnetic spectrum.

> "The future battlefield will be neither clean nor predictable. The framework aims to help British war fighters prosper amid the chaos of land battle by providing a conceptual handrail."

- **Reboot our approach to sustainment to make it fit for the 'Precision Age'.** The reach and accuracy of contemporary and future fires systems places the traditional approach to sustainment of most land forces in jeopardy. Concentration will be punished. So too, limited redundancy and resilience. A revised approach will need to draw upon dispersal, concealment, forward manufacture and repair, and low signature contracted support.[5]

- **Seize and maintain the initiative in the information environment.** Land forces must increase the speed, reach and sophistication of their information warfare capabilities to set the conditions for success before conflict, and to help shape perceptions nimbly if a crisis unfolds.

THE BATTLE WINNING FRAMEWORK

These five imperatives are embodied in what the Land Operating Concept terms the Battle Winning Framework. This seeks to fully internalise recce-strike, both deep and close, whilst also placing appropriate emphasis on protection and sustainment. It suggests that we win future land battles (within a joint context) by dislocating the enemy's offensive or defensive system at reach, and then rapidly exploiting the opportunity that this affords. Whilst at the same time avoiding friendly culmination, driven either by losses or the erosion of campaign authority. It would make sense to do this by making the deep battle as decisive as possible, and by principally using the close battle to shape for these deep effects.

This battle-winning framework is not a cast-iron prescription. The boundaries between its detailed steps described in the Land Operating Concept will be blurred, whilst some will take place concurrently and endure. Also, on occasion the circumstance may require a fundamentally different approach. That said, it has broad utility. The future battlefield will be neither clean nor predictable. The framework aims to help British war fighters prosper amid the chaos of land battle by providing a conceptual handrail. One that serves to emphasise: the importance of stand-off effects; the shaping significance of the close fight, prosecuted in or from complex terrain synthesising recce-strike with high-grade unit manoeuvre; and the foundational challenge of deploying, sustaining and fighting the force in a robustly survivable manner.[6]

It is worth stressing that it is not 'either/or' when it comes to future deep and close battle in the land domain. It is likely both, always, and at the same time. The relationship between the two will be symbiotic. Traditionally, deep activity has set the conditions for close success. Technology will increasingly provide land forces with an opportunity – albeit one that they will need to work hard to realise – to dislocate the adversary's fighting system at ever greater range and with increased confidence through fires and deep manoeuvre. To achieve this, significant shaping will need to take place by close combat forces. For instance, ground manoeuvre to prompt enemy find, fires and command and control assets to unmask. Or else the manoeuvre of intelligence, surveillance and reconnaissance and fires assets into a position where they can target adversary lines of communication. Or using defensive operations to force the enemy onto ground where they are easier to target. Here, close manoeuvre activity is setting the conditions for deep success, rather than the other way round.

That is not to underplay the importance of the future close battle. Just the opposite in fact. It will be fundamental to success. It is simply to suggest that, wherever possible, over time the close fight should increasingly be viewed through the optic of its contribution to depth dislocation and exploitation. This is not to imply that land forces will not sometimes win battles through a decisive act in the close battle. Indeed, on occasion it will be prudent to do so – or else we will have no

---

[5] *Success here will be especially dependent on wider Defence to gain Support Advantage. Defence Support's Advantage Charter and Action Plan contains some of the design principles and behaviours required for the future.*

[6] *In terms of the continuing, and expanded importance of the urban environment see Anthony King, Urban Warfare in the Twenty-first Century. John Wiley & Sons; DCDC's Global Strategic Trends: The Future Starts Today, (Sixth Edition, 2018); Future Cities Trends & Implications by Dstl and Louis A. DiMarco's seminal: Concrete hell: urban warfare from Stalingrad to Iraq. Bloomsbury Publishing, 2012.*

other alternative. After all, deep effects will often underperform. Not least, because the enemy will aim to aggressively contest the long range intelligence, surveillance, target acquisition and reconnaissance battle, whilst we will inevitably suffer attrition to our sensors, networks and precision stockpiles. Furthermore, there is a danger that the enemy will be able to generate more combat echelons than we have sensors or high-end, long-range weaponry to service.

All of this said, it is still prudent to try to win deep, and set the conditions to do so. We may fail, but the potential rewards are well worth the investment. Therefore, the conception of the close fight, setting the conditions for deep success, is a useful guiding principle with which to change tactical behaviours. And of course, in parallel we will strive to transform our approach to the close fight itself, through the increased fielding of stand-off find and strike assets all the way down to section level. This will allow battlegroups in the future Army a far greater opportunity to substitute attritional slugging matches for something more manoeuvrist.

"We will continue to think, experiment and adapt in response to the inevitable continued march of external change."

CONCLUSION

This briefest of introductions to the Land Operating Concept, and its attendant new way of winning, provides a sense of where we are and where we are going in force development terms. During the next decade, the Army will prioritise capability investment and force structural change to enable the deployed force to fight and operate in the manner described in the Land Operating Concept and précised above. It will also adjust its doctrine, education and training to slew the Army onto the new approach.

In parallel we will continue to think, experiment and adapt in response to the inevitable continued march of external change. And we will do so in the closest possible collaboration with the Royal Navy, Royal Air Force and UK Strategic Command, as well as NATO partners. After all, the land force is but a cog within a multi-domain and coalition machine. As much as anything else, the power of combinations will unlock the future land battle.

CHALLENGES OF MODERNISATION AND THE PATHWAY TO SUCCESS

AUTHORS

Colonel Chris Coton is Assistant Head Concepts in Army Headquarters. His previous appointments include Capability Planning in the Finance and Military Capability Directorate, and command of the Army's Medium Air Defence Regiment.

Dr Jack Watling is a Senior Research Fellow at the Royal United Services Institute and works closely with the British military on the development of concepts of operation and assessments of the future operating environment.

WHEN armies look to modernise, they often reflect on their past attempts at transformation. When the US Army embarked upon creating Multi-Domain Operations,[1] it modelled its efforts on General Donn Starry's development of AirLand Battle.[2] British discussions of Army modernisation invariably look back to the Haldane or Bagnall reforms. In all these cases there is a narrative of a clear, centralising and empowered figure driving rational changes in force design and equipment prioritisation.

Much of the narrative surrounding these modernisation programmes, however, is ahistorical, imposing a deliberate process backwards by extrapolating from a rational end result, and in doing so smoothing over how long, difficult and imperfect the process invariably was. AirLand Battle, for example, came from operational studies of the Yom Kippur War of 1973,[3] but was not accepted and adopted until 1982[4] and once published,[5] took until 1990 before most of the relevant capabilities were actually in service. The Haldane Reforms may have left Britain with the right first echelon to blunt Germany's advance alongside French allies in 1914, but it still left the British Army fielding large formations of horse cavalry and far fewer machine guns than was evidently optimal. Changing an army is hard. Liddell Hart's observation that "the only thing harder than getting a new idea into the military mind is to get an old one out",[6] has become a cliché precisely because it is uncomfortably accurate.

---

[1] *US Army, 'The US Army in Multi-Domain Operations 2028', TRADOC Pamphlet 525-3-1, 6 December 2018.*

[2] *Eric J Wesley, 'AUSA Global Force Symposium: Day 3 – Opening Remarks and Keynote Speaker', 28 March 2019, accessed 26 May 2019.*

[3] *The first iteration being Active Defence, TRADOC, 'FM 100-5 Operations 1976', 1976.*

[4] *US Army Training and Doctrine Command (TRADOC), 'FM 100-5 Operations 1982', 1982.*

[5] *General Donn A. Starry, 'To Change an Army', Military Review 63 (March 1983).*

[6] *B. H. Liddell Hart, Thoughts on War, first edition, London, United Kingdom: Faber and Faber, 1944.*

The British Army has been attempting a process of recapitalisation and transformation since 2014. The realisation that large scale warfighting in Europe may once again threaten the UK's security led to a drive to regenerate a 'warfighting division'[7] in the 2015 Strategic Defence and Security Review following Russia's annexation of Crimea. At the same time, it was understood that emerging capabilities meant that it was necessary to not just regenerate a 1980s formation but to address new threats, from long-range precision fires and uncrewed systems to modern communications. This necessarily required a definition of what the force was trying to do in the 2030-2035 timeframe, to set the requirements for new platforms, alongside investment to ensure the recapitalisation of the current force. The half-life of the unsynchronised concepts and programmes intended to address these two imperatives is testament to how the Army has struggled to deliver a coherent pathway for the institution. Project Wavell and the resultant Land Operating Concept, endorsed by Defence in June 2023, has finally set an azimuth for modernisation. But it has taken 11 years for the Army to agree to a concept. The Army will require discipline to see through its implementation during the next decade.

This article aims to illuminate the challenges to army modernisation, how they have manifested during the production of the Army's new operating concept, and how the approach to Project Wavell has sought to contend with them. It seeks to provide a handrail for those force developers who will follow: a guide to illuminate the pitfalls of modernisation and offer guidance for their survival. It is presented in two parts: first it will examine the difficulties of diffuse aiming points, the challenges of army pluralism and finding consensus, and the perennial issues of army conservatism; then it will offer four methods that Project Wavell has deployed to mitigate these – convincing audiences that there is a problem, building an evidence base, securing internal and external advocacy through communication, and securing credible and visible commitment from top-level leadership.

"The inherent need to adapt to an uncertain future means that prioritisation, rationalisation, and hard bets all carry significant risk. The problem of course is that without making bets, a force will lack the resources to modernise effectively."

PART ONE: WHY IS CHANGE SO HARD?

Diffusion. Reaching agreement about the future structure and capabilities that a force needs is complicated by uncertainty and diffusion of purpose. This is born in part from the difficulties inherent in predicting future wars. There are numerous examples in history in which armies have endeavoured in peacetime to determine how the next conflict will unfold, only to be surprised by the ensuing reality. France's military concepts following the First World War are perhaps the best example. Even where armies have managed to accurately foresee the next war, the opening battles have tended to present surprises.[8] Sir Michael Howard famously argued that "whatever doctrine armed forces are working on now, they have got it wrong... what matters is their capacity to get it right quickly when the moment arrives".[9] But the inherent need to adapt to an uncertain future means that prioritisation, rationalisation, and hard bets all carry significant risk. The problem of course is that without making bets, a force will lack the resources to modernise effectively. Because optimising for an envisioned future is inherently risky, there are always good arguments for hedging across an army's constituent branches, and yet this hedging collectively eliminates the resources necessary to modernise.[10]

The issue of a diffusion of purpose preventing optimisation decisions is particularly acute for the United Kingdom. For the Ukrainian or Israeli militaries, for example, there is but one relevant adversary and this is a stable planning assumption. The environment within which they must optimise their force is also known and unchanging. As an island nation the deployment of land forces for the UK is always discretionary. That does not make deploying land forces less likely, of course; as an instrument of policy the British Army is called upon regularly. But it does mean that it is very difficult to predict what a future British government will use the force for with a high degree of confidence. As an institution this drives a desire to retain any existing capability 'just in case'. To give a tangible example there has been an ongoing debate within the Royal Artillery about the merits of wheeled or tracked guns. The relative merits of these systems are context dependent. So long as the planning assumption remains ambiguous, therefore, the answer will be 'both' even if resources will not stretch to both at a sufficient scale.

Dissent. Armies of democratic nations tend to reflect the pluralistic nature of the society that they serve. Diverse opinions and debate are positively encouraged, with army sub-communities invited to contribute to the vision of the organisation that they serve. Extending the parallels with democratic societies even further, army modernisation is more complex than buying new 'stuff'; it is an ideological struggle to redefine how, where and with what the army fights.[11] Building consensus for such ideologies is fraught with challenges, and new ideas are frequently met with resistance. The first of these challenges is agreeing assumptions. As we have seen, armies have a poor track record in accurately predicting the future. This means, in a pluralistic community like an army, the future is up for debate. As Sir Lawrence Freedman observes, "prediction is often purposive, closely bound up with advocacy, and so is about the present as much as the future".[12] So stakeholder communities can, wilfully or otherwise, shape an army's vision of the future according to their respective equities. This could be to protect the status quo: "Often leaders who see their particular weapons becoming obsolete... are the most ritualistic and compulsive about the older forms of military command."[13] Or it could be (due to a lack of confidence to challenge with alternative approaches) a blind but well-intended reactionary pursuit of political zeitgeist. Either way, the end result is often perceived as indecision. Diversity of thought will

---

[7] *'National Security Strategy and Strategic Defence and Security Review 2015', p. 28: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf, 18 July 2023.*

[8] *David Barno & Nora Bensahel, Adaption Under Fire: How Militaries Change in Wartime (New York: Oxford University Press, 2020), 2.*

[9] *Michael Howard, "Military Science in an Age of Peace," RUSI Journal, vol. 119, no. 1 (March 1974), p. 7.*

[10] *Daniel Kahneman, Thinking Fast and Slow (London: Allen Lane, 2012), Chapters 31-33.*

[11] *Kurt Lang, Military Organizations, in Handbook of Organizations, James G. March, ed. (Chicago: Rand McNally & Co., 1965), 843.*

[12] *Lawrence Freedman, The Future of War: A History (Great Britain: Allen Lane, 2017), 286.*

[13] *Morris Janowitz, Sociology and the Military Establishment (New York: Russell Sage Foundation, 1965), pp. 102–103; Howard, "Military Science in an Age of Peace," p. 5; Meese, "The Process of Organizational Change," 105.*

always be encouraged – but it produces plenty of friction.

Dogma. The effectiveness of an army is ultimately determined by the will of its personnel to risk their lives to achieve the state's objective. This demands psychological optimism: soldiers must convince themselves that their equipment will work and that their tactics are effective. This necessary belief, however, makes it difficult for armies to accept that their capabilities or approach need to be changed. Armies are generally protective of their institutions and adopt a dogmatic approach to modernisation when compared with their counterparts in either the public or private sectors.[14] They instinctively prefer incremental change over deeper reform[15] and have historically resisted the adoption of new technologies, particularly those that have challenged their core identities.[16] In 1890, the great naval strategist Alfred Thayer Mahan reflected that "improvements of weapons [are] due to the energy of one or two men, while changes in tactics have to overcome the inertia of a conservative class".[17] Similarly, if somewhat more provocatively, Norman Dixon described the characteristics of military incompetence to include "a fundamental conservatism and clinging to outworn tradition", "a tendency to reject or ignore information which is unpalatable or which conflicts with preconceptions" and a "failure to use or a tendency to misuse available technology".[18] Armies are particularly conservative where change is concerned, as the risks associated with getting it wrong are generally existential.[19] Put another way, when technological evolution prescribes new ways of fighting, armies and nations are largely under a remit to get it right first time – or face annihilation.[20] Any attempt to modernise the force must contend with these conflicting tensions.

> "The project has set out to underpin top-level decision makers' confidence... this has required synthesis of hundreds of historical studies, evaluations of future technologies and threat analyses. And has involved physically testing hypotheses."

PART TWO: PAVING THE WAY FOR WAVELL

Convince. Project Wavell first dealt with convincing internal and external audiences that there was a problem: that the Army's ends, ways and means were not adequately in balance. It recognised the underpinning importance of clarifying why change was necessary, in a way that resonated with the organisation.[21] But a qualitative case for change would always be susceptible to differing interpretations, conservatism or simply a low tolerance for any change at all. In the Army's case, where bold decisions would be required to reset the balance of investment, an additional catalyst was needed. Then Russia invaded Ukraine. The nation was suddenly faced with a tangible and imposing threat of future war, narrowing any diffusion of its Army's purpose. The prospect of the next war has always tended to drive modernisation: "Change encounters less obstacles shortly before the outbreak of a war... a danger sensed by all muffles the voice of intrigue, and the innovation appears as a smaller evil that must be accepted to avoid a greater."[22] And thus the case for change could be built around the imminence of war in Europe. It served to set the conditions for Project Wavell's definition of the problem to be accepted internally.

Collect. As we have seen, there is invariably aversion to change in armies. To overcome such inertia, Project Wavell recognised that what was needed was a convincing logic trail, supported by empirical evidence obtained from the widest range of independent sources. The project has set out to underpin army top-level decision makers' confidence, and to unhinge cynicism or interventions from often well-intentioned parties who may lack their

Collect: Casualty evacuations using heavy-lift drones were among the novel techniques examined during this year's Exercise Wessex Storm.
UK MOD © Crown copyright 2023

[14] *Greenwald, Bryon E. The Anatomy of Change: Why Armies succeed or fail at transformation. Institute of Land Warfare, Association of the United States Army, 2000, 14.*

[15] *Barno & Bensahel, Adaption Under Fire, 231.*

[16] *Raphael Cohen, et al., The Future of Warfare in 2030: Project Overview and Conclusions, (Santa Monica: RAND Corporation, 2022), 8.*

[17] *Alfred Thayer Mahan, The Influence of Sea Power upon History, 1660–1805 (Novato, Calif.: Presidio Press, 1987), 20.*

[18] *Norman F. Dixon, On the Psychology of Military Incompetence, (London: Jonathan Cape Ltd., 1976), 152.*

[19] *Barno & Bensahel, Adaption Under Fire, 231.*

[20] *Scharre, Paul. Army of None: Autonomous Weapons and the Future of War, (New York: London: W.W. Norton & Company, 2018) 94.*

[21] *Chinn, David, and John Dowdy. "Five principles to manage change in the military." McKinsey on Government: Special Issue on Defense (2014): 40-44.*

[22] *David G. Chandler, The Campaigns of Napoleon (New York: Macmillan Publishing Co., 1966), 9.*

own evidence, or who might be pursuing a particular agenda. This has required synthesis of hundreds of historical studies, evaluations of future technologies and threat analyses (including interpreting those lessons from Ukraine that can most reliably be regarded as harbingers of the future), and commissioning over 20 'new' research papers where there were gaps in knowledge. It has involved the execution of dozens of wargames and red-teaming studies, including the largest Army wargame in living memory. And it has involved physically testing hypotheses with the Army's new Experimentation and Trials Group, whilst drawing similar insights from our closest allies and from our sister services. The approach has required discipline, consistency and patience, but has founded the Land Operating Concept on a recognised basis of empirical evidence.

Canvass. Establishing consensus, for all the reasons described in part one, has been challenging. Project Wavell has embarked on a campaign of incremental communication, to a broad set of both internal and external stakeholders. Externally, the approach has enlisted the assistance of well-respected defence think tanks – including Chatham House, the International Institute of Strategic Studies, and Royal United Services Institute – and a broad base of academia and technology consultants, including the defence industry. These bodies and others have allowed the Army to secure wide-ranging advocacy for both the approach and its content. Internally, the aim has been to reach the widest representative community – across the spectrum of rank, specialism and experience – to develop hypotheses, represent feedback and encourage ownership. The Army has been accused of introducing 'big bang' ideas for change in the past, surprising audiences with seemingly half-baked propositions. There is some sympathy for this approach, given the grinding realities of securing consensus, but Project Wavell has deliberately sought to 'drip feed' its hypotheses, rather than inflict an 'overdose' at the eleventh hour. The result has been greater buy-in through a form of federated ownership.

Champion. In his book on military innovation, Stephen Rosen describes the need for senior officers to personally champion change.[23] These officers must have established themselves by satisfying the traditional criteria for performance, to disassociate them from the agents for change who might otherwise be considered as 'mavericks' and be victim to sceptics. US General Donn Starry, in his acclaimed 1983 article on modernising the US Army, went further: "Someone at or near the top of the institution must be willing to hear

Open communication: A three-day British Army Expo, held at Wellington Barracks in London during July, highlighted how the Service's mobilisation and modernisation programme is progressing, and outlined its vision for the future. Courtesy of Soldier Magazine © Crown copyright 2023

out arguments for change, agree to the need, embrace the new operational concepts and become at least a supporter, if not a champion, of the cause for change."[24] Project Wavell has been fortunate to benefit from the establishment of a British Army Futures directorate stood up in 2021 specifically to champion and advocate change, and the Chief of the General Staff describing the new Land Operating Concept as "the foundation for our doctrine [that] enables us to prioritise both long-term investment and capability development; the idea that enables us to foster the intellectual edge required to succeed in war".[25]

STAYING THE COURSE

This article has exposed why change is so hard for armies, reflecting on the experiences over the last two years of Project Wavell and the production of the Army's new Land Operating Concept. It has set out the inhibitors of change and their longevity: the diffusion of purpose for armies compelled to offer limitless choice; the dissent born from an internal pluralism that in turn drives an internal ideological struggle; and the dogma born of institutional preference for tried and tested over novel approaches, given the cost of failure. The article has described how Project Wavell has endeavoured to build a consensus about the problem and therefore the need for change. It has also outlined the extensive evidence base that has been developed in underpinning Wavell's hypotheses. However, it is important to note that publication of the Land Operating Concept is merely the first step in driving appropriate changes into the British Army. Its successful implementation – realised through changes to the Army's doctrine, its structures, its equipment, its people, its infrastructure, and how it trains – is paramount. With a force development cycle now emphatically put in motion, the opportunity to get it right is tangibly close.

Seeing through the modernisation of the British Army is now primarily a question of institutional discipline. It takes years to bring capabilities into service. The risk is that more events lead the Army to 're-look' at its concept prematurely. While such updates might refine or adjust, they will also delay implementation and risk the force never actually following through. Wavell is not perfect, but if what it delivers is sufficiently flexible, it will be close enough once delivered. The process is also likely to be frustrating for troops. When AirLand Battle was published, US Army units had to practice the new way of fighting on their old equipment for years. When the German Army embarked upon mechanisation its tank crews spent years pushing around model carts to simulate armoured tactics.[26] But in both cases the willingness of the force to not make the development of tactics and doctrine beholden to the arrival of equipment prepared them for the next conflict. The key thing for the British Army now is to stay the course, to be consistent with itself and with the Ministry of Defence, and to translate its concept into capabilities fit for the future.

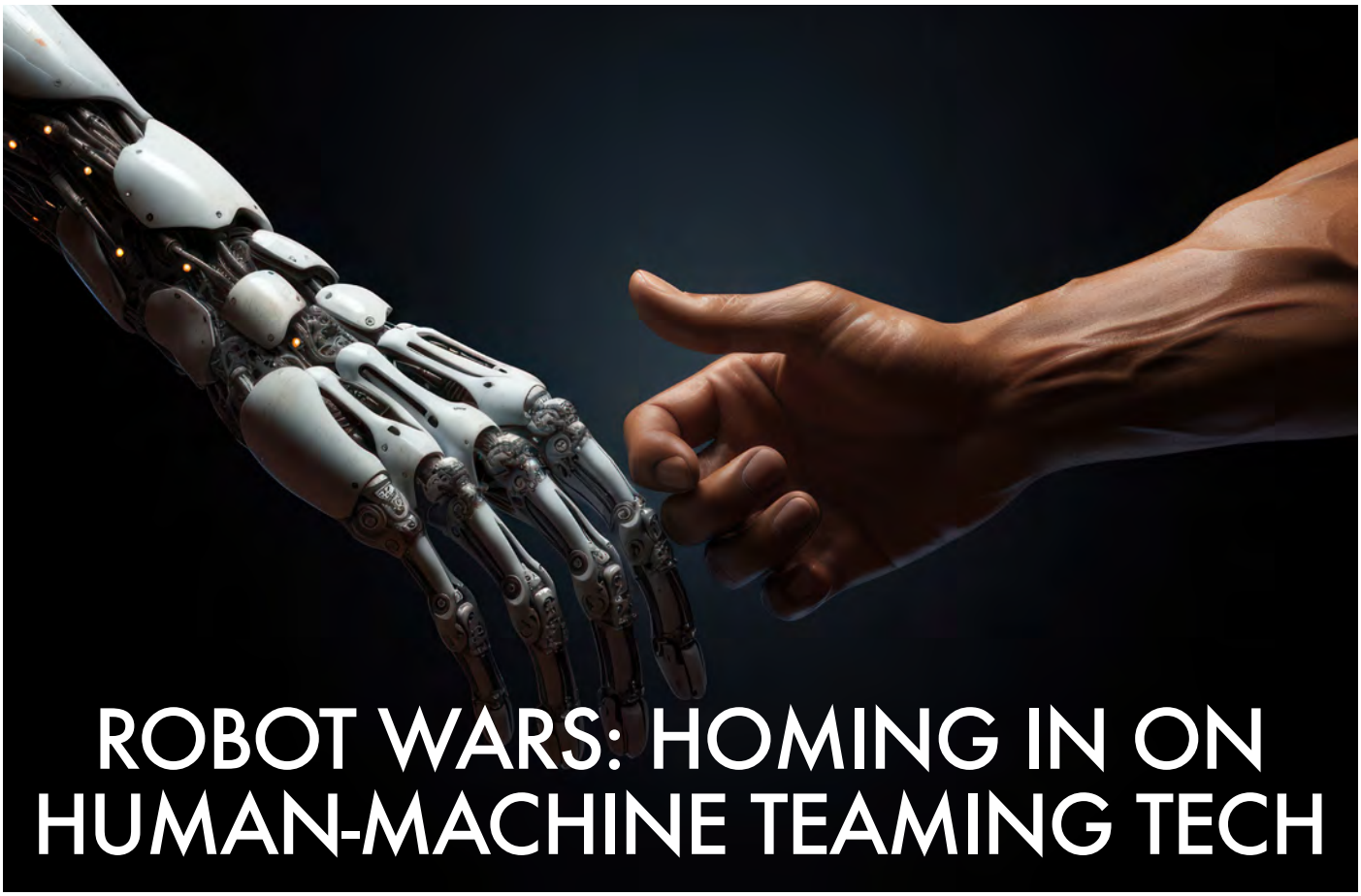
---

[23] *Rosen, Stephen Peter. Winning the Next War: Innovation and the Modern Military. Cornell University Press, 1991, 76.*

[24] *Starry, To Change an Army, 98.*

[25] *British Army, The Land Operating Concept – A New Way of Winning, (British Army: 2023), 2.*

[26] *Heinz Guderian, 'The Era of the Dummy Tanks: Military Sovereignty', Achtung Panzer!: The Development of Tank Warfare (London: Cassell, 1999).*



ROBOT WARS: HOMING IN ON HUMAN-MACHINE TEAMING TECH

AUTHOR

Colonel Tim Wright is a US Army Officer who has commanded a battalion in the 2nd Cavalry Regiment and holds a PhD in Political Science from the Massachusetts Institute of Technology. He is currently serving as a US Exchange Officer in Army Headquarters, where he is Assistant Head of Research and Experimentation in Army Futures, and the lead for the Human-Machine Teaming and Artificial Intelligence projects.

WHILE the Land Operating Concept acknowledges that the future of warfare is difficult to precisely predict, there are some clear signposts. One very evident signal is that robotic and autonomous capabilities paired with humans will exponentially increase the effectiveness of the British Army. The Human-Machine Teaming Project within Army Futures is an initiative to realise that – not five or ten years down the road but today. To achieve such an ambitious goal, we are experimenting with robots and machine learning, and novel ways of driving new capabilities into the Service at pace and scale. Though we have yet to fully realise our goals, we believe we are well on our way to delivering new capabilities for our soldiers, new approaches to acquiring technology, and new ways of fighting and winning on the battlefield.

In 2020, the Chief of the Defence staff made a speech in which he stated that 30,000 robots could be working alongside British soldiers by 2030. Looking around the headquarters at the myriad, disparate research and experimentation projects running at the time, it was clear we were well off the pace. Work was being done but it lacked the size, scale and coherence necessary to achieve such an ambition. There was no system or structure in place to generate robots (drones and autonomous systems), much less a programme of the type that enables the Army to acquire and deliver tanks, helicopters or radios. What's more, we lacked a clear understanding of the robots needed, where we would get them and what we wanted them to do. Finally, and perhaps most importantly, the world of robotics and autonomous systems was moving and changing at a lightning pace. Things that were cutting edge in the spring of 2020 were passé by the autumn of that year.

What's more, the character of warfare was shifting. As articulated in the Land Operating Concept, the British Army of the future will have to adapt and adopt a new way of fighting. In response to a crisis in Europe, the Army must be ready to engage an advancing enemy from the start of a conflict. It must cover more ground, operating in smaller, dispersed units rather than large, concentrated ones. With less manoeuvre mass, it will need the ability to find and strike targets at an increasing range whilst maintaining a small, difficult to detect signature. Proliferation of sensors will enable better targeting, yet it will also saturate every level with more targets than they can strike. No longer will a unit's higher headquarters be able to share its strike capability. Every unit must be able to solve its tactical problems at its own level. To meet such a challenge, every unit and every soldier must become significantly more effective, and robotics and autonomous systems will be critical to achieving that goal.

THE PROBLEM

To introduce such systems at pace and scale to the British Army, change was needed. First, if we attempted to use the traditional processes for acquiring capability, technology was going to leave us behind. The acquisition system, in rough handfuls, expects all the requirements for a new vehicle or system to be defined in advance and in great detail, describing exactly what characteristics incoming equipment will have so that it can meet the needs of the Army in the future. Once that conceptual blueprint is approved, companies compete to fulfil the requirements and for selection to build the capability. The chosen supplier will then start producing the equipment at small scale to ensure it does as it should. Once a final design has been determined, production at scale commences ahead of delivery to the Army. Historic (and recent) experience shows that this process takes, at best, seven to ten years to put a capability into the hands of soldiers. Not only does it take a long time, but the longer it takes the more likely it is that the capabilities defined at the start of the process will not match the requirements the Army has at the end. Lastly, projections of cost, performance and time made at the beginning of the project rarely match reality when it is over.

Applying this procurement model – one optimised for large, expensive capabilities that the Army will keep in service for decades (such as tanks and artillery) – to robotics and autonomous systems was unlikely to prove successful. Such systems rely on software to deliver their competitive advantage, not hardware. As a result, evolution in this field moves at the speed of software updates and programmers' fingers, cycling in months not years. If one had tried to use the acquisition system to buy mobile phones in 2013, we would have had to envision 2023, define and lock in our requirements, and find someone to make them. As a result the Army would today be receiving iPhone 5s as consumers on civvy street began un-boxing their far more sophisticated iPhone 14s. Furthermore, there is a vast market of companies constantly competing to provide better software-based systems for military use. Firms no longer rely on government contracts to innovate and develop new capabilities in this sector, they are investing their own resources and energy. As a result, no company sits at the top for long. Committing to a single supplier to provide such technology is, therefore, neither necessary nor prudent. We needed a process that operated differently.

Whatever new process we adopted, it not only needed to adapt to changes in the market but had to increase the Army's understanding of what these systems could do and where they would best enhance battlefield effectiveness. In brief, it needed to generate a base of knowledge from which the Army could operate as an informed consumer of technology. While the Army generates excellent generalists, officers and soldiers who can go into most situations and bring value, it does a poor job of creating specialists, those that have deep knowledge in a single area. Personnel change postings on two-to-three-year cycles, so even specialists rarely focus on a single problem for very long. Therefore, the Army needed a stable team that could provide expertise and continuity over time to ensure prudent acquisition of capability.

> "Evolution in this field moves at the speed of software updates and programmers' fingers, cycling in months not years."

Lastly, to achieve an ambition of 30,000 drones (or even 3,000), we had to pursue this capability as an integrated system rather than individual pieces of equipment. The most important components of autonomous platforms are not the bits of carbon fibre flying through the air or the machine moving along the ground, but rather the software that enables all of these systems to communicate and interact with each other. Whilst a single person flying a single drone with a single screen is useful, the only way we get to soldiers increasing their effectiveness on the scale required by the Land Operating Concept is through controlled autonomy: one soldier, one screen but multiple systems fulfilling multiple functions. A software backbone is critical and it must operate at scale. To achieve an integrated network of systems, small-scale experimentation was not going to work – we needed a large-scale partner to make this happen.

THE SOLUTION

To address these challenges and introduce robotics and autonomous systems into the British Army at pace and scale, Army Futures established the Human-Machine Teaming Project to conduct – in partnership with 16 Air Assault Brigade – large scale experimentation. Providing experimental capability for immediate use in operational contexts, the project can deliver operational advantage now whilst also building knowledge and expertise in the field to de-risk future investment. If it evolves as planned, by 2025 the project will have created the first robotics and autonomous systems-enhanced brigade, validated a new approach to experimentation and acquisition, and accelerated the Army's transition to the future of warfare. Though three years is a long time in most contexts, it is a short sprint in the capability world. Therefore, the project is focussed in its approach and scale, innovative in its structure and culture, and laser sighted on the critical next steps to the Land Operating Concept.

The Human-Machine Teaming Project established and remains guided by a set of operating principles that discipline ambition while maximising learning by doing. First, the project prioritises and focuses its efforts on the critical capability requirements where we believe robotics and autonomous systems will have the greatest operational advantage at battlegroup level and below in support of the Land Operating Concept. Specifically, these

UK MOD © Crown copyright

technologies should increase our ability to:

- Find, acquire and validate targets – and strike them – at every level;
- Deliver assets with increasing levels of autonomy, including lethal/non-lethal effects;
- Provide increasingly precise friendly asset visibility and status;
- Enable system integration through data collection, transfer and processing across a software backbone.

Second, robotic and autonomous systems that deliver these capabilities are determined and differentiated by the power of their internal software, systems and processes. Therefore, the project is focussed on software over hardware, and – following the lead of major international tech companies – employs a software-centric development model. Briefly, the project seeks out diverse capabilities (such as small unmanned aerial systems, sensors and user interfaces) that are readily available and best-in-class now, integrates them into a functioning capability and then pushes them to users as soon as possible. Rather than trying to identify and work out all of the details and bugs prior to issue, it allows users to experiment, test, break and innovate with systems to better inform refinement and improvement of the end product. The data gathered through use informs system updates and the cycle can be run again and again. If things break along the way, that is fine, as long as learning is achieved.

> **"Rather than trying to identify and work out all of the details and bugs prior to issue, [the Human-Machine Teaming Project] allows users to experiment, test, break and innovate with systems to better inform refinement and improvement of the end product."**

The third principle follows from the second – we cannot afford to execute such a cycle with highly expensive, exquisite systems. This approach is not suitable for £10 million tanks or £100 million aircraft, but it can be done if we focus on systems that are small, cheap and plentiful, and built for the generalist user. By focussing on software rather than hardware, we have de-emphasised the importance of the platform. Scoping to the generalist user prioritises simplicity, which makes it easier to attain mass, over the higher-end exquisite, where cost becomes a limiting factor.

Lastly, and perhaps most importantly, none of this delivers the operational advantage we need on the modern battlefield unless it is a fully integrated system of systems operating across a network that enables data collection, transfer and processing. Artificial intelligence, machine learning and advanced analytics are the most direct path towards the exponential increase in soldier effectiveness demanded by both Future Soldier Next Steps and the Land Operating Concept, but these capabilities are useless if our systems do not communicate. Though it is easy to simplify this problem to one of radios, bandwidth and power amplification, the true challenge is getting diverse software systems to interact, pass data amongst themselves and present it to human users in useful ways. Therefore, the core of the Human-Machine Teaming Project is the development of a software integration backbone that is robust to future demands and agnostic to bearer and processor and enables every level to efficiently and effectively pass the data that is critical on the modern battlefield.

STRUCTURE

To achieve this, the project is built on a novel structure that is providing a model for future investment in robotics and autonomous systems. It is led by a team in Army Futures, which sets the objectives, adjusts its direction, and guides it onto the headmark established. To provide commercial expertise, interface with the market and continuity within the project, the Future Capabilities Group at Defence Equipment & Support established the Expeditionary Robotics Centre of Expertise. This specialised group of commercial officers, researchers and managers controls the novel commercial framework that facilitates an equipment purchasing cycle that runs in months, multiple times a year. This framework has moved tens of millions of pounds worth of capability over the last financial year and maintains a headroom of £300 million for the life of the project.

These two components, while critical, do not overcome the lack of subject matter expertise, technical skills and knowledge of the market that are endemic to military acquisition. To overcome this gap, the project has appointed a systems integrator, Rowden Technologies. The company's role

Courtesy of Soldier Magazine © Crown copyright

is not to sell us a product but to provide us a service – specifically, systems integration capability. Rowden ensures data can flow across disparate systems and that every bit of equipment purchased gets delivered to the user as an integrated capability. It also provides expert advice on the technology we pursue, informing the direction both of experiments in the short term and the objectives of the project in the long term. However, none of this work matters if we do not learn from it, which is why we have a data management partner in IBM UK. The IT firm oversees the collection, analysis and curation of the data from the project, all of which is Ministry of Defence-owned. Furthermore, it leverages its vast resources to work specific data-related problems to accelerate progress towards greater autonomy and increased soldier capability.

Finally, the Field Army provides two critical partners for the Human-Machine Teaming Project: the Experimentation and Trials Group and 16 Air Assault Brigade. The former is an invaluable resource; charged with generating knowledge on the tactical future of warfare, it validates all the equipment capability generated, ensuring that when it reaches 16 Air Assault Brigade, it is fit for use. The Group also uses capabilities to conduct experimentation on the future tactics and tactical organisation of ground manoeuvre forces, exploring the impact of technology on the Land Operating Concept. It is with 16 Air Assault Brigade that experimentation at scale is truly achieved. As the project increases its output, the Brigade will receive ever more integrated and capable equipment. While experimental, the additions will provide increasing operational effect as they continue to be refined.

By the time our work culminates in April 2025, the expectation is that the robotics and autonomous systems delivered by the Human-Machine Teaming Project will allow 16 Air Assault Brigade to:

- **Extend its offensive range from 8km to 25km through:**
  - Unmanned sensors providing find, acquire and validate capability, operating in swarms;
  - Loitering munitions/one-way attack providing an extended strike reach in denied environments;
  - Network/AI-data processing supporting accelerated decision making from platoon to battlegroup level.
- **Expand defensive frontage covered by a factor of five (3km to 15km) through increased offensive ranges and enabled by:**
  - Heavy UAS/log leader follower – increased/automated sustainment assets;
  - Network – extended range of communications capability.
- **Increase survivability through:**
  - Greater dispersal enabled by networks, extended resupply, and find/strike at every level;
  - Multi-spectral signal reduction.
- **Accelerate decision making enabled by:**
  - AI-enhanced data processing and common operating picture;
  - Integrated network support;
  - Real time, multi-dimensional asset visibility.

UK MOD © Crown copyright 2023

CHALLENGES

Approximately one year into the project, much progress has been made. The commercial framework is up and running, the systems integrator and data partner are performing beyond expectations, and there is genuine learning and experimentation underway. The Experimentation and Trials Group has proved to be an invaluable partner in driving change and has demonstrated its value as a critical component of Army Futures' exploration of the future of warfare. The project is about to enter its second round of competitions, primarily focussed on software capabilities built around autonomy and artificial intelligence. Inevitably, there have also been some wrinkles, as one would expect with such a novel approach.

Ultimately, the Human-Machine Teaming Project is helping the Army to deliver integrated robotic and autonomous warfighting capabilities – that make a difference on the battlefield – into the hands of British soldiers. These are not future capabilities, they are available and exploitable today, and Army Futures is doing its level best to accelerate their delivery as a critical first step towards making the Land Operating Concept a reality.

CASTING ASIDE THE CRYSTAL BALL: PUTTING WARGAMING AT THE HEART OF FORCE DESIGN

AUTHORS

Colonel Nick English is Assistant Head Strategy and Force Design in Army Headquarters. His previous appointments include Capability Planning in the Finance and Military Capability Directorate and command of an attack helicopter battlegroup.

Paul Elrick is Dstl's Chief Land Analyst and has more than 30 years of experience in delivering operational research studies in support of Defence Force Development.

"Making a wrong decision is excusable, refusing to search continually for learning is not."
*– **Philip B. Crosbie***

PREDICTING the future has a history – a history woven with both remarkable insights and profound failures, and one that makes force development a wicked problem. Without certainty over any potential turns in the road ahead, what should the Army be designed to do and how should it do it?[1] In the face of shifting policies and priorities, how do we generate the confidence necessary to make force design interventions?

As we discuss in this edition of *The British Army Review*, our response to the conundrum has been to take an inductive approach to force development through Project Wavell. The British Army and others have amassed a huge body of knowledge, evidence and analysis. We have used this as the basis for developing a vision for how land power delivers relevant political choice in the future. Whilst this is in itself necessary, it is not sufficient. Once you have a theory, you must test the implications. When you employ a force, will it perform as you think? How will it respond to different adversary choices? How do you best balance the inevitable trade-offs in force design? What should you spend your money on to achieve the greatest impact?

This article describes how we have put wargaming at the heart of force development and used an analytical campaign to deliver an iterative approach to concept and capability development. It will outline what we mean by wargaming and how we employ analytically robust techniques to develop insights into the future. These techniques underpinned Army Wargame 23, the largest force development wargame run by the Service in living memory. Coming at the end of a two-year campaign of analysis, this capstone, 11-week event employed more than 250 analysts and players, from multiple providers, to explore the capability implications of the Land Operating Concept. Some of the conclusions will be familiar, some will be a surprise. All offer insights that can shape future force design on the basis of evidence rather than simply staring into the crystal ball and hoping for the best.

WHY WARGAME?

"It is a capital mistake to theorise before one has data."
*– **Sherlock Holmes***

Wargaming is experimentation. Whilst lots of valuable experimentation takes place in the field, it is very difficult to generate a controlled and representative environment against which we can test and refine new ideas. Analytical wargaming is different: it is not about winning or losing, it is not a simulation, and is not a means

of predicting the future. It gives us the ability to model and test again, and again, and again, at relatively little cost with a wide range of different dynamics at play. Conducting force level experimentation using computerised and manual wargaming results in more evidence of higher quality because more options can be assessed at a greater scale and with greater control of key variables. These tools are designed to assess the relative performance of alternative options, not predict a precise outcome.

Whilst they may appear similar, there is a significant difference between wargaming and the large-scale constructive simulations that we use in training.[2] Rather than deliver a rich and dynamic training experience tailored to the blue force, analytical wargaming is designed to be complex and repeatable. This requires models and tools that are underpinned by analytically robust and assured data and rules. This ensures that experiments are credible, repeatable, transferable and – critically – meet His Majesty's Treasury's criteria for investment quality evidence.

The Defence Science and Technology Laboratory (Dstl) has developed a wide range of models, techniques and data sets to support wargaming. WISE [Wargame Infrastructure and Simulation Environment] is a detailed computer-based tool used to assess warfighting performance up to divisional level. It has been used by Dstl to explore Army force development and capability investment questions for more than 25 years. In common with the other analytical models used to inform decision making, WISE must adhere to Dstl's software requirements which includes verification and validation testing.[3]

"Conducting force level experimentation using computerised and manual wargaming results in more evidence of higher quality because more options can be assessed at a greater scale and with greater control of key variables."

Not only are the model's underpinning algorithms designed and tested to ensure they appropriately represent real engagements, the performance data used within them is based on more detailed simulation models or trials. For example, the probability of kill for weapon systems is often derived from secret performance data obtained through live trials. Whilst one might imagine that wargaming is heavily computerised, this is not always the best technique for the research question being explored. Manual wargames are also a simulation of warfare and also undergo a process of validation. The Rapid Campaign Analysis Tool and High-Level Warfighting Wargame Manual have both been validated against real world examples. Most recently, the latter was validated against operations in Ukraine. This not only validated the baseline wargame but identified important aspects not previously represented that have now been incorporated.

However, just because a wargame technique has been validated does not guarantee that an experiment will successfully explore an analytical question. Wargame designers must ensure that focus areas are properly explored within the game. For example, there is no point simply increasing the mass of deep fires where any additional targets are out of range. Designers must also ensure that the metrics that they generate adequately explain the outcome

---

[1] *Brian W Head, Forty years of wicked problems literature: forging closer links to policy studies, Policy and Society, Volume 38, Issue 2, 2019, pp 180-197.*

[2] *Examples include Combined Arms Staff Training and the US Warfighter series of exercises.*

[3] *Verification and validation: Analytical quality assurance is more than checking that the analysis is error-free and satisfies its specification (verification). It must also include checks that the analysis is appropriate, i.e. fit for the purpose for which it is being used (validation). HM Treasury, The Aqua Book: guidance on producing quality analysis for government, March 2015.*

of the game. For example, does recording measures of force effectiveness such as systems losses, casualties or achieving the mission adequately characterise the impact of concept and capability changes?

Dstl uses an evidence framework to assess the strengths and limitations of the available evidence and answer the question: how much evidence is enough? The Evidence Framework Approach requires those who generate the evidence to objectively assess what they have produced according to five criteria and scores are assigned for each to determine if the evidence is weak, moderate, strong or beyond reasonable doubt. Within the Army Wargame the evidence generated was often judged as 'strong' because of the robust analytical approach employed across the five following criteria:

- **Comprehensiveness** – the wargames were specifically constructed to explore the Land Operating Concept in the context of Euro-Atlantic escalation. Within all the wargames the behaviours (actions) of both sides could be explained. When variations were explored, such as increased uncrewed air systems, fires or ground-based air defence, their impact could be directly understood.

- **Relevance** – the scenario was taken from the endorsed Defence Scenario Book. It was further developed through Defence level Planned Force Testing wargames and additional analysis from Defence Intelligence and other agencies.

- **Challenge** – all the wargames were adversarial in structure. The adversary was played by experienced Dstl and industry red players familiar with threat capabilities and doctrine. Unlike training exercises, the red force was never constrained to allow the blue force to use certain capabilities or enhance the training benefit. In addition, Dstl employs an independent technical reviewer to challenge study design and ensure that the study's findings are valid for the techniques employed.

- **Quantity** – the Army Wargame used a campaign of multiple wargames coupled with previous relevant studies to increase the evidence quality. Previous wargames, with alternative threats or schemes of manoeuvre, in different terrain coupled with evidence from relevant past (and current) operations all contributed.

- **Veracity** – given the baseline and associated variations, e.g. increased deep fires, were chosen due to insights identified in controlled environments it was relatively straightforward to identify any game outcome change and the effect that caused it.

"There is no silver bullet, no killer insight, no single investment that can transform how the British Army successfully counters a peer adversary. This is a battle of systems, to survive on a future battlefield you can't afford gaps that your adversary can exploit."

THE ARMY WARGAME

"The great tragedy of science – the slaying of a beautiful hypothesis by an ugly fact."
*– **Thomas Huxley***

In partnership with Dstl, Army Futures developed a two-year programme of wargaming and operational research that culminated with Army Wargame 23. This allowed us to test nascent ideas as they were developed and create a rapid feedback loop between concept development, force design and force testing. We were able to flow ideas out into defence, UK Strategic Command and US Army Futures wargaming, test them in joint and multinational contexts, before flowing them back into the Army programme.

The Army Wargame tested a future force employing the Land Operating Concept across four mission groups[4], with a focus on combat operations in the Euro-Atlantic set in 2030. This design allowed us to harness critical thinking well beyond the normal boundaries of the British Army, with contributors including Dstl, QinetiQ, the Royal United Services Institute, the International Institute for Strategic Studies, Chatham House and US Army Futures Command. Whilst it is challenging to operationalise a concept that hasn't yet been embodied in doctrine, breaking the problem into a series of sub-games or pulses allowed us to progressively expand from the tactical to the theatre and operational level.

WHAT DID WE LEARN?

"All models are wrong, some are useful." – ***George Box***

The Army Wargame was a deliberately tough test. In many ways it represented the land component's worst-case scenario. This allowed us to take the force to breaking point and identify those insights with the strongest evidential basis. By changing our approach and optimising some of our capabilities, we found we could improve the performance of the force by an order of magnitude.[5] This was achieved by tilting the board in our favour: taking a different approach to readiness, setting the theatre through campaigning and fighting differently. Whilst the detailed capabilities insights are understandably classified, we can signpost where the high payoff capability interventions might lie. Firstly, it quickly became clear that there is no silver bullet, no killer insight, no single investment that can transform how the British Army successfully counters a peer adversary. This is a battle of systems, to survive on a future battlefield you can't afford gaps that your adversary can exploit. If you enter the battlefield with a gap, your adversary will find and exploit it. To win, we must combine both different ways of fighting and different capabilities, but we don't need to wait for a future equipment programme to deliver new capabilities into the hands of soldiers. The ideas of the Land Operating Concept can be employed with the equipment we have now. This is the approach the US Army employed at the introduction of AirLand Battle, making a conceptual shift ahead of equipment programmes delivering.[6]

Secondly, speed confers strategic advantage. The ability to react quickly presents a strategic dilemma to an adversary that is likely to exploit the grey space ahead of a NATO response to achieve their strategic outcomes. Readiness is less defined by 'notice to move' but much more by 'notice to effect'. This has a significant impact on those capabilities that have the most impact and where they are positioned and places a premium on strategic and operational mobility. It is not sufficient to have capable equipment, it must be able to have an effect in time to deliver relevant political choice. This implies that hard to move, heavier equipment needs to be close to potential points of use and follow-on forces are more likely to be mounted on wheels. The capabilities that added the most value quickly were command and control, long-range fires, attack aviation and air defence.

Whilst speed is important, we cannot break the laws of deployment physics – but we can bend them. Defence and Army wargames have repeatedly demonstrated the difficulty of fighting on exterior lines, our supply chain quickly becomes our operational weakness. NATO theatre setting can offset first move advantage and forward positioning

---

[4] *Homeland protect and defend, deter and contain in the Euro-Atlantic, counter hostile state threats, and international engagement.*

[5] *Against a land component baseline of Planned Force Testing 7 in 2018. This used a similar but not directly comparable scenario set in the Euro-Atlantic.*

[6] *M1A1 Abrams, Bradley IFV, Patriot Air Defence system, AH64 Apache, and UH60 Blackhawk.*

pays dividends in both response time and endurance. Overall, our ability to sustain the force needs to be dispersed, protected and closer, prioritising the high payoff stocks such as long-range fires and air defence munitions rather than what we might otherwise be culturally drawn to.

Thirdly, the expanded battlespace changes how we fight. It will require a significant mindset change to accept dispersal and exploit porosity. Dispersal has real benefits, it makes the force harder to find and harder to kill. But whilst dispersal drives survivability it also increases complexity: the deep and the rear are often the same place, it relies on the echelon above to cover the gaps between the dispersed brigades, and it generates a different kind of logistic problem that places a real premium on logistic command and control. A point of inflection is also now apparent between divisions and brigades. At the Brigade Combat Team and below, we gain significant advantage from employing layered find and strike. Every layer must be able to see and strike further. An active counter sensor battle is as important, if not more important, than fighting a counter battery artillery duel. In many ways we can afford to be bypassed by a tank but not a drone. The data available from a drone allows a much wider range of systems to be brought to bear against us. The division is the point of cross domain integration, employing a greater proportion of rocket fires to target the adversary system across their depth. Increased range is used to fire from further back and makes it harder to kill rather than necessarily firing further.

Fourthly, the near surface is the new vital ground; our ability to contest and exploit the near surface defines tactical success. Increased lethality and survivability is linked to our ability to see and strike further. This applies at every level from the sub-unit upwards. Unsurprisingly given what we have seen in Ukraine, the proliferation of small unmanned air systems at the lowest level produced a significant payoff. Dominating the near surface, however, is not simply about employing more drones. Fighting an effective counter sensor battle is essential. We must fight a much more aggressive counter sensor battle employing both air defence and capabilities such as Ajax in a covering force to deny target data to an adversary.

Finally, we must layer capabilities through the force to increase resilience and make every part of the force increasingly capable. Increased lethality and range at the battlegroup level complements our ability to see and strike further. This requires capabilities such as 120mm mortar, a range of near surface lethal and non-lethal drones, and access to ground-mounted complex weapons. We must also make every artillery round count for more. Reducing the number of rounds to achieve an effect has a disproportionate benefit as it ripples back through the supply chain. We have ten years of wargaming data that demonstrates the impact that technologies such as sensor-fused munitions can have on our overall effectiveness. Whilst we require robust command, control, communications, computers and intelligence at the battlegroup level to prevent tactical fragmentation, fighting in an electronically-contested environment is hard. The lifeblood of cross-domain integration is data and a division is likely to remain the right level to hold the mass of human knowledge, skills, and experience to exploit it.

INTO FORCE DESIGN

"I don't want the truth; I want something I can tell Parliament!"
*– **Rt. Hon. James Hacker, MP [Yes Minster!]***

"Data is a precious thing and will last longer than the systems themselves."
*– **Sir Timothy J. Berners-Lee***

Concept development, force testing and force design are never ending. Wicked problems don't stop, they are not solved but re-solved again and again in different ways. By running a programme of robust analysis iteratively with concept development and force design, we have been able to test capability implications in a much more coherent and consistent way than we have ever done before. The Land Operating Concept has delivered the ideas that underpin the force design that the Army Wargame has tested. Whilst the insights generated are not facts, they are produced in a way that is evidentially robust and accepted across Government to support investment decisions.

The insights and data from the Army Wargame will flow directly into the development of an Army Baseline Force design. This will determine what changes we must make to fully deliver on an army that is designed to fight and designed to fight differently. It is not the answer but is an answer, and an answer based on the best evidence that we have. The Army Wargame will deliver a final pulsed wargame this autumn. This will test the Future Soldier force design against the new baseline force with a view to identifying those high payoff force design interventions that the Army should pursue now.

UK MOD © Crown copyright 2023

THE FALSE LESSONS OF MODERN WAR: WHY IGNORANCE IS NOT INSIGHT

AUTHOR

William F. Owen (Wilf) is the co-founder and Editor of *Military Strategy Magazine*. He is a former infantryman and has worked as a Command, Doctrine and Capability contractor.

*"The fool believes that the tallest mountain in the world will be equal to the tallest one he has observed." – **Nassim Taleb***

THE aim and purpose of this article is to highlight the problematic phenomena of journalists, academics and even soldiers who seek to identify lessons from current or recent conflicts when few, if any, of these things should be noteworthy given a professional land warfare community that is sufficiently informed.

If the British Army were knowledgeable about land warfare, almost none of these lessons would qualify as insight. Lessons should be a product of analysis, not observation. Observations have often been wrong. The very word lesson implies a certainty that is often unsafe or overstated. The word insight is preferable. A real lesson should suggest a non-discretionary changing of training, doctrine, organisation or capability beyond the currently recognised understanding. While called "lessons", today's use of the word strongly implies novelty and revelation of previously unknown things, thus dramatic and revelatory.

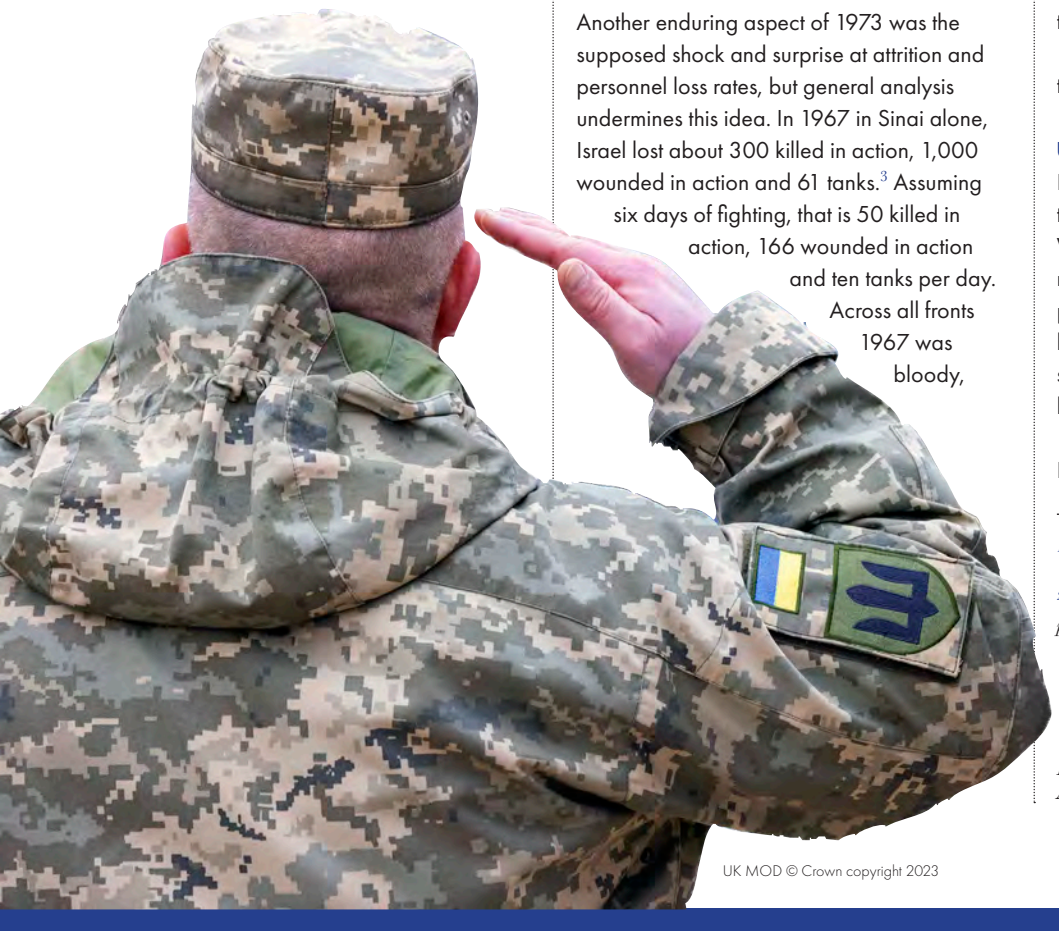
Warfare in the Russo-Ukraine War is two to three generations behind the standard competent, well-trained armies should aspire to operate. There should be few lessons for the well-informed student of land warfare. Most claimed lessons are about equipment capabilities couched in terms the general public can understand because of the desire for internet traffic and clicks. The widely cited opinion does not equate to useful or correct. The desire for public traction means discussing main battle tanks occupies far more text than fuel handling or road and track surface maintenance. The errors creep in when British Army officers, policy makers and civil servants believe that something is new when it is not because it leans against evidence-based analysis and understanding. An Iranian Shahed 136 drone is conceptually not much different from a Second World War V1 and easier to kill.

THE LESSONS OF 1973

In 1990 Anthony Cordesman and Abraham

Wagner produced a three-volume work entitled *The Lessons of Modern War*, to which was added a fourth volume in 1996 to account for the Gulf War of 1991. The previous volumes covered the Iran-Iraq, Arab-Israeli, Falklands and Soviet War in Afghanistan. Given the near-legendary levels of insight and revelation the world gained from Israel's 1973 War and the subject of the first volume, it would seem fair to suggest that some 17 years later, in 1990, the lessons would have been well understood. Much was less than certain, yet paradoxically, a book written in 1978, Trevor N Dupy's *Elusive Victory*, had got far more right than later writers were to get wrong.

The significance of Israel's wars in 1967, 1973, and, to some extent, 1982 cannot be understated in the literature of modern warfare because, almost uniquely among 'Western nations', Israel implemented lessons from conflicts it fought. Therefore the 'lessons' of these wars became extant in decisions Israel took and funded. In contrast, much of the literature defaulted to narratives such as the end of the tank and how shocked the Israel Defense Forces had been by the Egyptian AT-3 Sagger missiles. Yet within two years of the end of war, an Israeli general let slip that their analysis showed that anti-tank guided missiles accounted for only some 25 per cent of main battle tank losses.[1] There was also the fact that Israel had a more advanced anti-tank guided missile in service in the shape of the Nord SS-11, which it held in a corps level anti-tank reserve unit mounted on M3 half-tracks. The idea that the anti-tank guided missile was a conceptual surprise to the Israel Defense Forces has to be seen against the context that they had purchased such weapons before Egypt had.



"Why should the lessons from Ukraine be removed from the specific context of the participant's differing training and equipment levels and be relevant to the British Army? Is something that is a lesson for the Ukrainians a lesson for everyone else?

The idea that the tank was dead was especially fallacious. Post-war, Israel procured more tanks, not less, but also increased the size of its army. The story that in 1973, the Israel Defense Forces were tank-heavy with not enough infantry and artillery is a myth. In 1973 they had 50 tanks battalions, 50 infantry battalions and 55 artillery battalions. In 1982, they had 90, 80 and 80, respectively, albeit in total numbers, and the artillery tubes were close to 120 unit equivalents.[2] Thus the idea that Russia is a 'fires-led army' has to be considered against the fact that as of 1982, the Israelis certainly were and that fires lead manoeuvre in contrast to the opinions of the 'manouverist approach'. Lots of 'lessons' from 1973 continue to be either wrong or the Israelis learned different lessons from those the rest of the world saw.

Another enduring aspect of 1973 was the supposed shock and surprise at attrition and personnel loss rates, but general analysis undermines this idea. In 1967 in Sinai alone, Israel lost about 300 killed in action, 1,000 wounded in action and 61 tanks.[3] Assuming six days of fighting, that is 50 killed in action, 166 wounded in action and ten tanks per day. Across all fronts 1967 was bloody, with 176 killed per day and 407 wounded. In context, the United States Marine Corps averagely suffered 174 killed in action per day at Iwo Jima. In 1973 the total loss was 2,222 killed in action and 5,600 wounded in action, but the loss rate was 117 killed in action per day. Notably, 40 per cent of all Israel Defense Forces losses occurred within the first four days of fighting. In terms of equipment, Israel started the war with 2,100 main battle tanks. It lost about 1,100 but recovered and repaired all but 410. The Israel Defense Forces also lost 102 combat aircraft (a loss rate of five per day), with the overwhelming majority falling to surface-to-air missile systems.

Simply put, no conflict today comes even close to these types of losses, yet the myth persists that war and warfare are becoming 'more lethal'. They are not, and a large body of literature proves it.[4]

If you take those as lessons, then the development of the NATO AirLand battle concept can be argued as an outcome of the lessons of 1973, yet NATO did not sow minefields or dig anti-tank ditches along the inner-German border. On the Golan Heights, the Israelis did. Nor did NATO pursue the development of long-range indirect fire anti-armour systems. Israel did. Nor did NATO focus the same amount of attention towards unmanned air systems and the air and land forces' suppression of enemy air defence. The Israelis did. In some sense, NATO and the US decided on the lessons and learnt them regardless of what the Israelis did. NATO applied lessons in a NATO context. Context trumps lessons and insights. As the lessons of 1973 make clear, the idea of 'lessons' is less than clear-cut.

UKRAINE

Fast forward to today and the war in Ukraine; there is far less to be learned than in 1973. Why should the lessons from Ukraine be removed from the specific context of the participant's differing training and equipment levels and be relevant to the British Army? Is something that is a lesson for the Ukrainians a lesson for everyone else?

In 1973, most Israeli units were as well trained

---

[1] *Herzog, Haim. War of Attonement 1975.*

[2] *"War without End" – Lt Col Eado Hecht, IDF .ppt presentation used on numerous British Army Battlefield Studies.*

[3] *Dupuy, Trevor. Elusuve Victory page 279.*

[4] *See the collected work of Trevor N Dupy and Christopher Lawrence. Understanding War, War by Numbers and Attrition*

as NATO and with more direct combat experience in armoured warfare. Secondly, almost everything used by Israel was in front-line NATO service at the time and most relatively new and state-of-the-art.

In sharp contrast, the current war in Ukraine sees much-outdated equipment in ad-hoc combat formations, not seemingly underpinned by NATO equivalent training, doctrine and organisation levels.

As of June 2023, no main battle tank in Ukraine has a fully integrated sensor and active self-protection system, which needs to be contrasted against the number of times Israeli active protection systems have defeated modern Russian rocket-propelled grenades and anti-tank guided missiles. There is no reported use of modern high-altitude long-endurance or medium capability unmanned aerial systems with high-performance payloads able to generate CAT-III/IV target data at greater than 50 kilometres. Except for Brimstone, there is no reported use of long-range non-line-of-sight anti-armour systems. Neither side seems to be fielding modern IP-based battle management systems using multiple bearers and self-forming networks. What does exist seems improvised, but if not, where are the insights? All these things have been common in the modern Israel Defence Forces for more than a decade and machine learning and staff automation tools are already being fielded.

Likewise, the integrated defensive aid suites on Israeli AH-64s have consistently defeated man-portable air-defense systems, making helicopter losses in Ukraine far less relevant as an observation. The Russians have had an equivalent system offered for export for more than a decade. Notably, this has attracted very little comment.

Interest in the combat performance of individual platforms such as the Leopard 2A6 would carry very little in the way of insights if it weren't operated by crews with the training expected of the observer. Notably, 'training' and 'command competence' feature very little in the claimed Ukraine lesson literature. In sharp contrast, the US Army's National Training Center cites its existence as 'lessons learned' from 1973 and Israel Defence Forces combat training.[5]

DRONES AND THE TRANSPARENT BATTLEFIELD

As most admit, drones are nothing new but the 'transparent battlefield' has been with us for a long time dating back to at least World War I and observation balloons directing long-range artillery. In terms of a more direct comparison to the Bayraktar TB-2 drone, Israelis made widespread use of similar though smaller and less detectable unmanned aerial systems to locate and target Syrian surface-to-air missile sites in 1982. The Israeli unmanned aerial systems could stay aloft at 15,000 feet for more than seven hours, broadcasting real-time images of the missile locations. They also performed electronic intelligence missions. In widespread use since Vietnam, drones were a well-accepted, well used and well-employed system by Israel in 1982, yet the Falklands War was fought with no such systems so where was the lesson?

> **"Why the impact of drones is so over-emphasised compared to the impact of far older technologies such as battlefield surveillance radar or unattended ground sensors is not clear."**

The claim that the war in Ukraine marks a step change in mass employment of small drones misses an element of 'so what' rigour. The average DJI Mavic Drone can transmit 5.1K video and can operate for 45 minutes out to 15 kilometres, so it has about 15 minutes on station at maximum range and is limited to 21 knots of wind. It uses 2.4 and 5.8 Ghz control channels. The military equivalent works out to only about 10 kilometres but spends 45 minutes on station. The critical difference is that the electro-optical/infra-red payload can detect NATO standard targets in darkness at 15 kilometres and humans at 10-12 kilometres and generate target data sets. It also uses military communications with a far lower probability of detection, jamming or intercept. They can also operate with no control link, recording footage and returning to a safe area to downlink it. This is just quad-copter-type unmanned aerial systems.

In Ukraine, what is being reported as 'lessons' are capabilities over a decade or more in the past. Simply put, the most advanced and capable small military drones currently in common use are not present in Ukraine in any way that has impacted current battlefield observations. Why the impact of drones is so over-emphasised compared to the impact of far older technologies such as battlefield surveillance radar or unattended ground sensors is not clear. It seems likely that since many civilians can purchase the same drones, there is a vicarious attachment to commenting on a capability with which they feel familiar. Battlefield video also reinforces that perception.

Good camouflage and concealment defeat most of the current civilian drone capability, so a standard of training that would mitigate low and slow flying Fiesler Storch in 1940 would substantially be simple and easy to implement and was routine in the British Army of the Rhine from 1945 to until the early 1990s. As most soldiers know, simple countermeasures can render thermal imagery far less effective than commonly supposed.

BIGGER PROBLEMS

For two reasons, seeing lessons in Ukraine, or 'signposts for the future of war', is substantially problematic for the British Army. The first is that the British Army had a useful and valid understanding of contemporary warfare long before the Russian invasion of Ukraine in February 2022. This understanding informed the Strike Tactical Doctrine in 2017 and built on a wider body of work that dates back to the early 1960s when tactical nuclear weapons drove the need for dispersion.[6] The strike brigade concept proves that the British Army was across the problem long before February 2022. That said, much good work was limited by extant platform choices, lack of funding and failures of previous programmes. A speech made by the current General Officer Commanding 3rd (UK) Division at the RUSI Land Warfare Conference 2019 stated that the British Army was on the right track.[7] Notably, the core observation confirmed the need to train to fight dispersed and the training challenge it presented. As yet, few, if any, observer in the Ukraine conflict has talked about training or methods of operations, yet it is central to a British Army warfighting approach. The war in Ukraine validates the controversial strike brigade dispersion and signature reduction issue. It is not a lesson from it. The strike brigade was conceptually and doctrinally well prepared to fight the war that had occurred.

The second problem is that of equipment and budget. The claim that the war in Ukraine demonstrates X or Y capability need for the UK is mostly reputational or obvious to informed observers. Some claims may also be wrong. This creates the inference of a pressing evidence-based case when such a case is either already well understood or wrong. The

---

[5] *How to train an Army Podcast – Peter Roberts.*

[6] *The author of this article worked on Strike Tactical Doctrine.*

[7] *Brigadier James Martin, RUSI Land Warfare Conference 2019 – Session Five.*

UK MOD © Crown copyright 2023

public's desire to talk about tanks when air defence and electromagnetic warfare may be more pressing further skews the debate. The risk is that the 'lessons of the Ukraine war' become a Trojan Horse for bad ideas and a poor understanding of combat power. Why would the war in Ukraine produce any more insights than the six-week-long second Nagorno-Karabakh War of 2020, where it could well be argued that both sides were better equipped and trained than the combatants in Ukraine? Nagorno-Karabakh saw the widespread use of loitering munitions. Still, these have existed for more than 35 years, have been used in multiple conflicts, and have generally been more advanced in capability than those used in Ukraine, so their employment holds little insight.[8]

BAD IDEAS

The conception that current conflicts somehow provide insights into future conflict regarding things that an army can prepare for today is neither as safe nor historically valid as many assume. For example, the British Army's choice to mechanise completely in 1927/28 was not a direct lesson of any conflict.[9] The British Army had experimented with mechanisation well before World War I. Likewise, it is extremely debatable to suggest that the defeat of the British Expeditionary Force, once the French Army collapsed in May 1940, resulted from a failure to learn the lessons of World War I or even the Spanish Civil War. In terms of capability, far more British Army equipment proved either adequate or ideal in terms of what was designed before the war as was found wanting. Many of the problematic ideas about tanks were extant well before the war and based mostly on the personal opinions of men such as JFC Fuller and other members of the armoured 'avant garde'.

The future is unknowable. The idea that things happening in wars today provide some insight into what war will be like tomorrow is sound and logical but only valid and useful if subjected to analytical rigour and placed in the organisational, cultural and practical context, often reducing the relevance of insights. For example, little is written about the British Army's lessons from the US experience in Vietnam compared to the Israelis in 1967 and 1973.

The primary insight to be gained from observing contemporary conflicts is that of preparedness for war. Can you do the things that are needed to win battles and engagements? The fact that Russia or Ukraine is firing an X-amount of 155/152mm shells per day is not a lesson. It may be irrelevant to the British Army if those forces are not as well trained as the British Army or able to leverage the intelligence, surveillance, target acquisition and reconnaissance and command, control, communications and intelligence integration, which the British Army should have in service, meaning each round fired is substantially more effective. The British Army has fought and trained to fight wars where high artillery ammunition expenditure was and is a fact. It cannot, therefore, be 'a lesson of modern war'. Observations from Ukraine or any other conflict need to be placed in regard to the context of your force's training and overall education. If it's something you know or did, it is not a lesson.

CONCLUSIONS

There is considerable danger in seeking to see and write about lessons from ongoing conflicts in the belief that, axiomatically, there must be lessons from all on-going conflicts. This view is contestable. Many find that idea surprising or even ludicrous because they are unfamiliar with the corpus of the British Army expertise apparent in the recent past. The British Army has a strong corporate memory of preparing to fight major European land wars. That is not trivial.

The British Army's inability to deliver land equipment programmes and control its own budgets does not detract from the fact that well before both the Nagorno-Karabakh War and the Russo-Ukraine War, the Service had a largely correct and validated understanding of modern warfare based almost entirely on basic professional rigour which observations of the war in Ukraine validates rather than challenges. While not without problems, that model has little to learn from the war in Ukraine, given that at least five years before the Russian invasion, the British Army was preparing to fight a Russian Army substantially more competent than the Russian Army apparent today.

---

[8] *The IAI Harop entered service in the IDF in the mid 1980s and was briefed to the UK as a potential UOR in the 1990s.*

[9] *JP Harris, Men Ideas and Tanks.*

WHY REPELLING RUSSIA REQUIRES AN ASYMMETRIC APPROACH

AUTHOR

Brigadier Gerhard Wheeler is an adviser to the Foreign, Commonwealth and Development Office. During his previous service as a regular British Army officer he held a number of operational command appointments, including command of a multinational force in Afghanistan and a battlegroup in Iraq.

Acknowledgements: Lieutenant General Jonathon Riley CB DSO PhD, Director, Generalship; Brigadier Ian Thomas OBE, Dean of Studies, Royal Military Academy Sandhurst; Dr Mike Martin PhD, Director, Threshed Thought.

"History showed that there could be no single theory of strategy, correct for every age."
– Gordon Craig, ***Makers of Modern History***

WHAT form of warfare should the British Army plan to fight to deter Russian aggression in Eastern Europe? When it last faced a similar question in the latter stages of the Cold War, it plumped for the concept of manoeuvre warfare. That decision led to a revolution in how it thought about the development of its doctrine, capabilities and force design. But is manoeuvre warfare the answer for the challenges it faces today? To answer that question, it is worth comparing the theory alongside its sister concepts of attritional and positional warfare.

Although arguably a centuries-old idea, the theory of manoeuvre warfare enjoyed a renaissance in the 1980s. Faced with the threat of a Soviet Army that could mobilise millions of men in an armoured assault on Western Europe, US and UK military strategists looked for a plan that could provide an effective and credible form of conventional deterrence to avert an almost immediate and inevitable switch to nuclear weapons. Constrained by West Germany's policy of Forward Defence, which demanded that any military engagements be fought as far eastwards as possible, they chose a scheme that made the most of the advantages of their smaller but more technologically-advanced and professional land and air forces. The US led the charge with its AirLand Battle concept,[1] which was partly a rejection of its failed attritional campaign in Vietnam. The British Army took a similar approach under the leadership of Field Marshal Sir Nigel Bagnall. Bagnall's proposals mirrored the US AirLand Battle concept by advocating the need for a manoeuvre-oriented approach to military operations, focusing on agility, tempo and shock directed against the opponent's weak points rather than on set-piece, attritional and territory-oriented battles.[2] In both cases, a different relationship with the air forces was an inherent part of the concept and key to its success.

There are numerous competing definitions of manoeuvre warfare but in its simplest form it can be described as the use, or threat, of force to break the cohesion of an enemy. In

[1] *Gessert, Robert A, The AirLand battle and NATO's new doctrinal debate, The RUSI Journal, Volume 129, 1984 – Issue 2.*

[2] *Mader, Markus, In pursuit of Conceptual Excellence: The Evolution of British Military-Strategic Doctrine in the Post-Cold War Era, 1989-2002, 2004, p89.*

an armoured warfare context, it could include tactics such as flanking movements, infiltrations, penetrations of defensive lines, envelopments, encirclements, counter attacks, feints, diversions and deceptions; and attacks by ground and air-delivered weapons on the enemy's depth. In the right circumstances, such tactics can be highly effective because they have the potential to break the will of an enemy to continue fighting if the execution of the manoeuvre makes the enemy believe its situation is untenable. As such, manoeuvre warfare offers the promise of rapid success and, often, a reduced need to directly engage the enemy when compared with other forms of warfare.

The most famous successful example of manoeuvre warfare is the German Blitzkrieg of 1940: a deep armoured penetration which exploited the seam between two French armies and tore apart the Allies' defence of France and the Lowland countries. But other celebrated examples exist throughout history including General Edmund Allenby's decisive mobile campaign against the Turkish Army in Palestine in 1918 and General Douglas MacArthur's surprise amphibious landing at Inchon in 1952, which cut the supply lines of the Korean People's Army. The concept can however also fail, sometimes spectacularly. The German defence of the British-led airborne assault to seize the bridge at Arnhem in 1944 and the early stages of the 2022 Russian invasion of Ukraine both show that determined defenders who hold their ground, and respond with rapid counter attacks, can foil manoeuvre warfare tactics. It is therefore best used in environments where forces can move with relative freedom; where surprise can be achieved; and against an enemy whose morale is likely to collapse if the cohesion of its organisation or position is disrupted.

Attritional warfare focuses on the incremental destruction of the enemy's physical capabilities. Since the rebirth of the idea of manoeuvre warfare, the concept of attritional warfare has gained a reputation as an inferior and undesirable form of warfare. Associated in the popular imagination with the bloody stalemate of the Western Front in the First World War, it can be seen as a futile act. Its critics, in particular, point to the senseless slaughter of Verdun in 1916 and the German Chief of Staff General Erich von Valkenheyn's later justification that his strategy was to ensure 'that the forces of France will bleed to death'.[3] However, an attritional approach can be effective. Field Marshal Bernard Montgomery used it to secure his pivotal victory at the second battle of El Alamein in 1942, where he utilised the superior firepower of the British-led Eighth Army so that it "crumbled away" the defensive lines of the Axis forces.[4]

Attritional warfare is often used in environments or situations where outflanking manoeuvres have become impossible, such as during Operation Goodwood, Montgomery's attempted breakout from the Normandy beachhead in 1944. Restricted terrain, urban spaces, advances in technology and well-matched opponents can all force an attritional approach. However, attritional tactics can also be employed as a preferred option. For example, when a force is able to concentrate superior firepower and sees an advantage in eroding an enemy's physical capability to fight, such as during the initial US-led air campaigns in the 1991 and 2003 Gulf Wars. Attritional approaches can also be effective when an enemy is enticed into exhausting its resources on an inconsequential objective. Notably it has proved to work in defeating the political will of a government or its people rather than its forces, for example, the North Vietnamese campaign fought against the American-led forces in the Vietnam War.

Positional warfare is not formally defined in British doctrine but can be described as the use of force – through tactics, firepower or movement – to move an opponent from one position to another for further exploitation or to deny them access.[5] The Duke of Wellington fought a brilliant positional battle at Waterloo in 1815 when he exploited the reverse slope of a gentle ridge to protect the British infantry squares from Emperor Napoleon Bonaparte's artillery. For the defender, positional warfare can be more economical in the use of forces because it offers better odds through the use of protection and exposes an attacker to well-laid defensive fires.

In the modern period, positional warfare is often associated with the trench warfare of the First World War and the Iran-Iraq War but there are other categories. City sieges are a form of positional warfare that have become increasingly common as the world has become more urban. Examples include the battles of Sarajevo in Bosnia, Grozny in Chechnya, Fallujah in Iraq and Aleppo in Syria. The complexity of urban terrain can greatly multiply the defender's advantages as has been evident in the current war in Ukraine.[6]

---

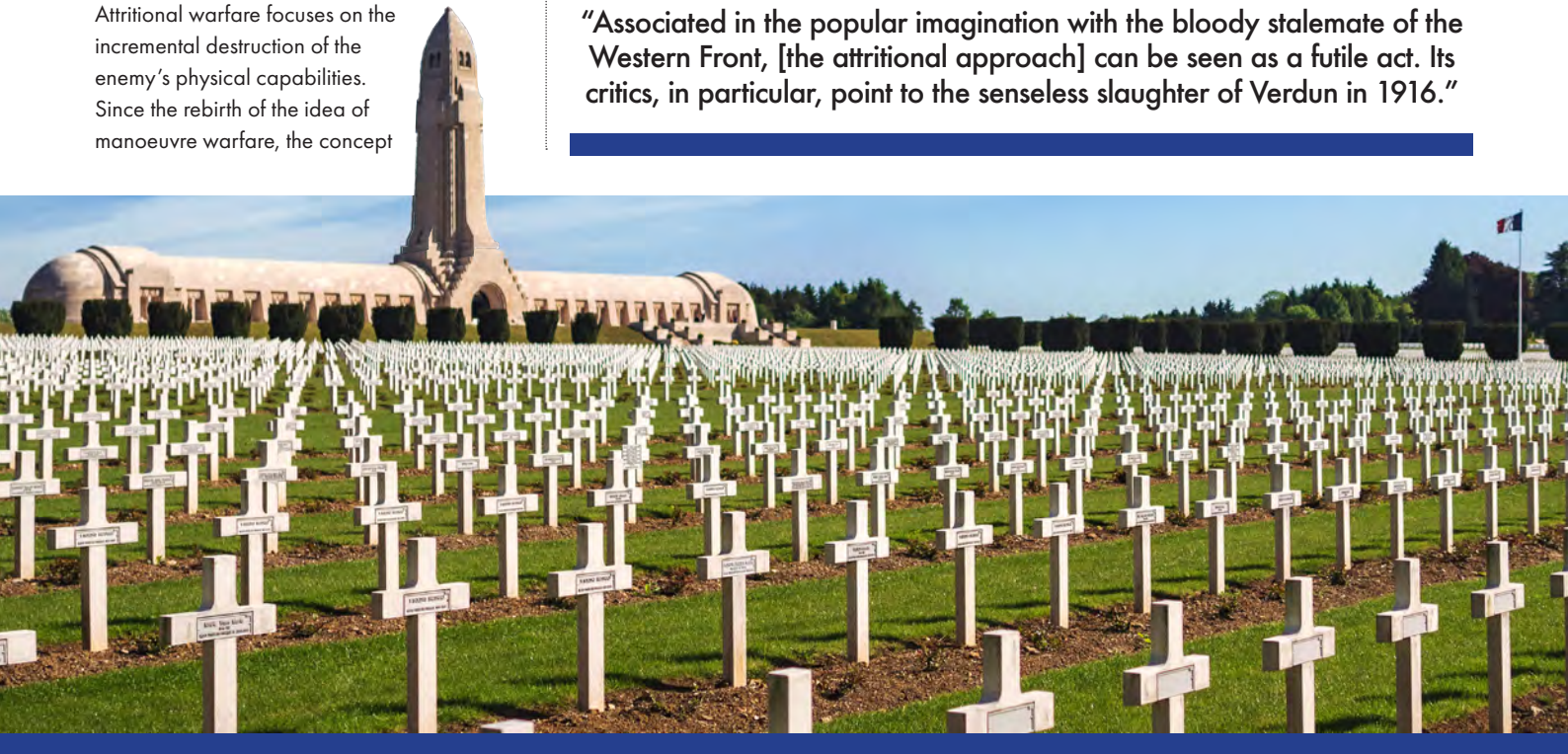
[3] *Falkenhayn, General Erich von, General Headquarters (1914-16) and its Critical Decisions, Berlin, Aug 1919.*

[4] *Carver, Field Marshal Lord, El Alamein to desert storm: Fifty years from desert to desert, The RUSI Journal, Volume 137, 1992 – Issue 3.*

[5] *Fox, Maj Amos C, A Solution looking for a problem: Illuminating Misconceptions in Maneuver-Warfare Doctrine, benning.army.mil, 2018.*

[6] *Nevertheless, as Stuart Lyle's excellent talk on urban operations myths to CHACR demonstrates the defender is not always advantaged by urban terrain. chacr.org.uk/2023/03/07/urban-operations-myth-busting*

"Associated in the popular imagination with the bloody stalemate of the Western Front, [the attritional approach] can be seen as a futile act. Its critics, in particular, point to the senseless slaughter of Verdun in 1916."



Another version of positional warfare, which has become increasingly associated with Russia's modern approach to warfare, is the rapid limited land grab designed to achieve a strategic fait accompli such as the illegal seizure of Crimea by Russian forces in 2014. A style of warfare that many had thought was consigned to history, positional warfare is very much back in fashion in the 21st century.

At this point, it is useful to highlight a common misconception about the use of manoeuvre in warfare. A force that manoeuvres should only be thought of as one that is engaged in manoeuvre warfare if it is manoeuvring as part of a plan to shatter the cohesion of the enemy. Whereas if it is manoeuvring as part of a campaign to incrementally erode the enemy's capability then it is waging attritional warfare; if it is manoeuvring as part of a scheme to seize key terrain then it is conducting positional warfare. Just because a force is exercising a flanking manoeuvre does not mean it is fighting a manoeuvre warfare battle. It is not the action that defines the form of warfare; it is the intended effect that counts.

In reality, outside of the confines of academic theory, most military forces employ a mix of all forms of warfare to prosecute campaigns. Perhaps one of the best illustrations of the three forms of warfare under discussion being used during one short campaign is the actions of the Egyptian and Israeli forces in the Suez Front of the Yom Kippur War in October 1973. The Egyptians began the war with a positional strategy: their surprise seizure of the Israeli-occupied east bank of the Suez Canal was designed to convince the US to restart diplomatic talks over the future of the Sinai and other areas occupied by the Israelis since the 1967 Arab-Israeli war. Their subsequent defensive battle, utilising anti-tank guided weapons and air-defence systems, was an attritional plan designed to blunt the expected armour-and-air counter attacks by the Israelis, which shocked the Israelis by its effectiveness. The attempt by the Israelis during the closing stages of the war to regain the initiative by driving armoured thrusts into the Egyptian Army's rear areas was a classic example of manoeuvre warfare; although it was only partially effective in breaking the Egyptian's cohesion by the time a ceasefire was called and so its effect was mainly attritional. Notably, Egypt's mix of positional and attritional warfare failed in its military objectives but did achieve its ultimate political objective: as part of a peace treaty, Israel agreed to return most of the Sinai a year later and handed back the remainder in 1982.

Given the pros and cons of the three forms of warfare, which is the best for today's challenges? The reflexive response from most of today's military professionals would probably be to select manoeuvre warfare. This is not surprising: in 1989 as a result of Bagnall's efforts to transform the British Army, the institution published its first formal doctrine.[7] It was, of course, aligned with Bagnall's thinking on the best way to deter the Soviet threat in Europe so was based on the theory of manoeuvre warfare. Soon afterwards it also adopted a new decentralised command philosophy – Mission Command[8] – that encouraged commanders to give their subordinates as much freedom as possible to exercise their initiative when interpreting orders; a style of command seen as key to enabling the fast pace of manoeuvre warfare. Ironically, this revolution in doctrine was published in the year that the Berlin Wall fell, which effectively ended the Soviet threat the rebirth of manoeuvre warfare was designed to counter.

The Army's warfighting doctrine has been developed since it was first introduced at the end of the Cold War. Its scope has widened the idea of manoeuvre to include virtual capabilities like cyber operations and it now accepts the need, at times, for attrition in war, but as its title suggests – The Manoeuvrist Approach[9] – it remains rooted in the philosophy of manoeuvre warfare. As a result, modern officers have literally been indoctrinated to think that any clever tactic is 'manoeurvist'. When one can now read a well-written blog that argues that Montgomery, the master of the set-piece attritional battle, actually fought a manoeuvrist fight at El Alamein it is clear that the label 'manouevrism' is no longer connected to manoeuvre warfare and has lost any useful meaning.[10]

Turning back to the problem of deterring today's Russian threat to Eastern Europe, we can see that the circumstances have changed considerably from the 1980s. Russia can mobilise a large army but nowhere as big as the Soviet war machine was once able to muster; the threat of follow-on forces that so exercised NATO's Cold War planners is now far less of a concern. Europe is even more urbanised and so manoeuvre is much harder. Technological advances have made it far more difficult for mobile forces to concentrate together or manoeuvre without being detected and broken apart by relatively cheap weapon systems. To devise a deterrence strategy to meet this threat requires an analytical approach that considers all conceptual forms of warfare rather than one that is skewed to prefer a manoeuvre warfare approach.

Instead of devising deterrence strategies and tactics constrained by manoeuvre warfare theory it would be wiser to adopt a capstone doctrine that accepts that all warfare is essentially asymmetric. It should articulate a universal approach that recognises that however similar opponents are to each other, there will always be differences in their resources, morale, strength, technology, resilience and other key factors, and so any contest will see each side look to pit its strengths against the other's vulnerabilities.

An asymmetric approach would not demand that a commander primarily focuses on breaking the moral or physical cohesion of the enemy. In some cases, that may not be the best enemy vulnerability to focus on. It might prove more effective to instead concentrate on reducing an enemy's military capability to fight or on seizing terrain or a domain that an opponent will find difficult to regain. Such a doctrinal approach would free commanders to devise strategies that can draw on combinations of manoeuvre, attritional and positional forms of warfare.

A doctrine based on an asymmetric approach could still use Mission Command as its command philosophy; the concept works just as well for positional and attritional warfare. And is ever more relevant in an era where denied and degraded communications must be assumed. However, the Army might need to adapt elements of Mission Command if it is going to depend more on mobilising its reserves for a conflict; this will mean considering how part-time soldiers can quickly integrate into a Mission Command philosophy. Delegating control and encouraging initiative can work well with citizen soldiers, as we have seen in Ukraine. However, presenting them with written orders riddled with jargon and abstract intention statements, stilted by a prescribed vocabulary of action verbs, may prove less effective than directives written in clear and concise English.

Returning to the original question of what form of warfare should the British Army plan to use to deter Russian aggression in Europe, it is instructive to look at a European country that has fought against Russia before and has for

---

[7] *Design for Military Operations, The British Military Doctrine, British Army, 1989.*

[8] *UK Land Power, Joint Doctrine Publication 0-20, Director Concepts and Doctrine, British Army, 2017.*

[9] *UK Land Power, Joint Doctrine Publication 0-20, Director Concepts and Doctrine, British Army 2017.*

[10] *Hebditch, Daniel, Second Battle of El Alamein – The Lost Manoeuvrist Battle?, Grounded Curiosity Blog, 10 Sep 2017.*

"Technological advances have made it far more difficult for mobile forces to concentrate together or manoeuvre without being detected and broken apart by relatively cheap weapon systems."

years since deterred further aggression without NATO allies. Finland, with a population of five million, has a small regular army of about 20,000 but is able to mobilise conscripted reserves of 180,000.[11] It has the largest artillery force of the democratic countries currently at peace in Europe.[12] Its concept of Total Defence[13] ensures that the whole of its society is integrated into its defence plans.

At the political level, Finland's deterrence posture has been, until recently, characterised by its neutral stance. But its military's strategic force design is optimised for an attritional war. Its military deterrence message is clear: the country is a fortress. Any aggressor would likely find itself fighting a long and costly war. At the operational level, Finland's Total Defence concept allows it to prepare its cities, critical infrastructure and geography to fight a positional campaign; it has even recently assigned rapid-response forces to counter Crimea-style land grabs.[14] At the tactical level it has elements of its force that are able to exploit manoeuvre warfare tactics; a skill it excelled in when its ski troops again and again outmanoeuvred and broke the cohesion of Soviet columns in the early stages of the 1939 Soviet-Finnish Winter War. Finland's deterrence strategy has been well crafted to apply its asymmetric advantages against Russia's perceived vulnerabilities.

The British Army is now reviewing how it can sharpen its competitive edge to contribute to Europe's deterrence strategy. That analysis, which will need to take in factors like tasks, culture, resources, technology, geography, allies and experience, will help it decide what combination of styles of warfare it should be structured to fight. This will drive force design. To illustrate from medieval examples, the horse-mounted armies of the Mongol Empire were ideally suited for manoeuvre warfare; while the high proportion of archers to cavalry in King Henry V's army at Agincourt dictated that it was best employed in an attritional battle.

The British Army's analysis will, no doubt, try to ensure it can fight all forms of warfare but inevitably it will need to shape its design more towards one style than others. If it decides that it is best weighted towards fighting manoeuvre warfare then its force design will need to prioritise capabilities that can disrupt the cohesion of the enemy, such as tanks, attack aviation and electronic warfare units; a force optimised for positional warfare will place greater demands on anti-access and area-denial systems, urban warfare units and rapid response forces. If it believes the best contribution it can make to European deterrence plans is to build mobile forces that can cause maximum attrition against the enemy's capabilities then it will need a force structure that is balanced more towards intelligence, surveillance and target acquisition systems; long-range fires; portable anti-armour and air defence systems; and distributed command nodes. For a small regular army, building stronger reserve force capabilities will probably need to be a course of action common to all approaches.

Whatever road the Army takes, it should now change its principal warfighting doctrine from a Manoeurvist Approach to an Asymmetric Approach. This would free commanders at all levels to be able to consider the most effective way to fight in any given situation. An Asymmetric Approach doctrine could provide them with the pros and cons of different forms of warfare and reinforce the values the British Army holds to in conflict, like avoiding civilian casualties, but not dictate a particular theory of war. Nested below this core doctrine could be theatre- or threat-specific doctrines and strategies as required.

In 1989 the introduction of a formal doctrine for the British Army was a big step forward in its professional development. It is now time to remove the dogma from its doctrine.

---

[11] *The Finnish Army, www.maavoitmat.fi*

[12] *List of countries by number of artillery, www.ArmedForces.eu*

[13] *Schultz, Teri, In Defense, Finland prepares for everything, www.amp.dw.com, 2017*

[14] *Peck, Michael, Finland's Unique Defense Strategy Makes it Ready for Anything, The National Interest, 2021.*

THE OPERATIONAL LEVEL OF WAR AND CAUTIONARY TALES FROM THE IRAQ CAMPAIGN

AUTHOR

Lt Jonathan Burden is a section commander in the Land Intelligence Fusion Centre.

TWENTY years after the start of the British involvement in Iraq, there are still major institutional lessons that can be drawn from the campaign with relevance for the future Army. This article examines the role of the operational level of war. By briefly outlining its genealogy within British doctrine and then applying it to the practise of strategy during two episodes of the Iraq campaign (the original invasion and Operation Sinbad), it reveals some of the limitations of the concept. The central thesis is consciously Clausewitzian and the article demonstrates that without rigorously embedding tactical action within a clear policy framework, the operational level can obscure the political dimension of a conflict with detrimental consequences for strategy. Critically, the evidence presented suggests a failure to address this concern will impede on future stabilisation campaigns.

THE OPERATIONAL LEVEL: STRATEGY AND MANOEUVRE

The origins of the operational level of warfare are variously traced to Napoleon, the Prussian Army of the 1860s or the Soviet Union in the 1930s.[1] The modern concept was first codified in Western military practice in 1982 in the US Army's *Army Field Manual 100-5, Operations* which defined the operational level as the 'theory of larger unit operations' and the 'conduct of campaigns' which is itself the 'sequencing of battles'.[2] More significantly the strategic, operational and tactical dimensions of war were codified as their own distinct levels. Yet as B.A. Friedman, amongst other critics of the concept argue, *Field Manual 100-5* 'mistranslated the Soviet version, conflated it with other

[1] *Epstein, Napoleon's Last Victory and the Emergence of Modern War (University of Kansas University Press, 1994); Freedman, Strategy: A History (Oxford University Press, 2015), 202. For a historical overview of the origins of the Operation Level in the Napoleonic, German, Soviet and American traditions see Friedman, On Operations: Operational Art and Military Disciplines (Naval Institute Press, 2021).*

[2] *This definition of campaigns is strongly reminiscent of the Clausewitz's definition of strategy as the 'use of battle for the purpose of war', Von Clausewitz, (trans.) Michael, Howard and Peter Paret, On War (Princeton University Press, 1984).*

"The limitations of linking strategy, operations and tactics via fixed levels with predictable links can be shown by turning to Clausewitz, who emphasised the chaotic and unpredictable nature of war due to it being an extension of politics."

concepts, misapplied it, and then accepted it without examination'.[3]

For the British Army, however, the concept reigns supreme. In a revealing essay, Lieutenant General Sir John Kiszely, former Director of the Defence Academy of the UK, argues the operational level provides the "vital link" between tactics and strategy and is where the "orchestration of military resources" takes place.[4] For former Chief of the General Staff, General Sir Richard Dannatt, it is the operational level "between [tactics and strategy] that is so critical, for this is where ideas are turned into practicalities. It is the level where the general really earns his pay because it is here that a plan is formulated that turns grand ideas into success achieved by forces on the ground".[5]

In contrast, for scholars such as Colin Gray, separating tactics from strategy is untenable. He argues that strategy exists to link tactical actions to policy goals, which are themselves the product of the political process.[6] For Kiszely, this role is played by operational art which he defines as an "activity: the linking of military-strategic objectives with tactical level actions".[7] Although this appears to be a minor or perhaps a minor semantic difference with Gray, the issue becomes clearer down the page when he argues that the "operational level is determined by where operational art is practised".[8] In the British system this is conducted by Permanent Joint Headquarters. Strategy has its own level embodied by the Government and the Ministry of Defence, rather than being understood as a practice or action. Although Gray does not explicitly argue for discarding the operational level (as others have), it is clear that an intervening level is harmful for his notion of strategy because tactics are logically severed from the political aims at which they are aimed at achieving.[9]

The limitations of linking strategy, operations and tactics via fixed levels with predictable links can be shown by turning to Clausewitz, who emphasised the chaotic and unpredictable nature of war due to it being an extension of politics. War is consequently characterised by uncontrollable violence, rather than being an extension of desired outcomes determined by policy and has a non-linearity that cannot be fought using simple, hierarchical relations.[10] The operational level, as a way of conceptualising war is therefore contingent on a particular, and likely wrong, understanding of its nature. Instead, scholars of strategy have articulated it as an iterative process that aims to realise evolving policies with available ways and means, emphasising the non-linearity, emergent properties and flexibility between tactics and policy aims.[11] Operational art in contrast, underpins the planning, conduct and sustainment of campaigns which are groups of tactical actions, intended to create political effect.[12] Operational art therefore enables the practice of strategy but it does not logically precede it.

Additionally, not long after the publication of *Army Field Manual 100-5*, the philosophy of 'manoeuvre' was adopted as the British and NATO way of war, in order to defeat the numerically superior Soviet Army. The 'Manoeuvrist Approach' sought to intelligently target the enemy's vulnerable centre of gravity to avoid a grinding attritional fight.[13] Nevertheless, despite being embraced to confront a specifically Soviet problem in a European theatre, the philosophy has remained broadly unaltered.[14] The consequent effect on strategy has been stark.

Hew Strachan claims that in contrast to 'traditional' strategy, which aimed to harmonise national policy and tactics, the operational level "occupies a politics-free zone" and by the First Gulf War was speaking in a "self-regarding vocabulary about manoeuvre, and increasingly 'manoeuvrism', that was almost metaphysical and whose inwardness made sense only to those initiated in its meanings".[15]

---

[3] *Freidman's recent polemic on the operational level argues that the Western adoption of the operational level has impeded the function of operational art, to the detriment of Western military practise. Friedman, On Operations.*

[4] *Kiszely, Thinking About the Operational Level, RUSI Journal, December 2005, 38.*

[5] *Dannatt, Leading from the Front: The Autobiography (Bantam Press, 2010), 122.*

[6] *Gray, Strategy and Politics (Routledge, 2016); Gray, The Strategy Bridge: Theory for Practise (Oxford University Press, 2010).*

[7] *Kiszely, The British Army and Thinking About the Operational Level, in British Generals in Blair's Wars (eds.) Bailey, Iron and Strachan (Ashgate Publishing, 2013), 125.*

[8] *Kiszely, Thinking About the Operational Level, 42.*

[9] *See Friedman, On Operations; Owen, The Operational Level of War Does Not Exist, Military Operations, Volume 1, Issue 1, Summer 2012, 17-20.*

[10] *Echevarria II, Clausewitz and Contemporary War (Oxford University Press, 2007); Kelly and Brennan, Alien, 94; Gray, The Strategy Bridge, 7. For a further discussion of the problems with fixed levels see Bruscino, The Theory of Operational Art and Unified Land Operations, School of Advanced Military Studies Theoretical Paper, Command and General Staff College, Summer 2012.*

[11] *Freedman, Strategy. Gray, Strategy Bridge, Echevarria II, Clausewitz and Contemporary War.*

[12] *Friedman in particular is keen to emphasis that operational art is an integral aspect of modern warfare but merging it with the operational level is problematic.*

[13] *Kiszely traces the emergence of the operational level of warfare and the philosophy of manoeuvre to the thought of scholars such as Brigadier Richard Simpkin and the patronage of Field Marshall Nigel Bagnall when he commanded NATO's Northern Army Group and subsequently became CGS. See Kiszely, Thinking About the Operational Level, 41. For a critique of the dominance of manoeuvre in American military doctrine, see Fox, Manoeuvre is Dead Understanding the Conditions and Components of Warfighting, The RUSI Journal, Volume 166, 10-18.*

[14] *ADP Land Ops, Army Doctrine Publication: operations (updated 31 March 2017) (publishing.service.gov.uk).*

[15] *Strachan, Direction of War: Contemporary Strategy in Historical Perspective (Cambridge University Press, 2013), 40.*

Lawrence Freedman makes the same point, stating that the operational level became a "politics-free zone where commanders could demonstrate their mastery of managing large forces over wide areas".[16]

This intellectual development was something of an unfortunate historical anomaly. Britain's long history of conducting small wars on the fringes of the empire had shown that: "Effective commanders had to be anthropologically and politically aware if they were to understand the dynamics of war in different regions of the globe. The 'operational level of war' tried to ignore this problem by treating the 'battlespace' as something to be shaped by common military doctrines [i.e. manoeuvre]."[17] Yet as Britain approached the Iraq and Afghanistan campaigns, there was a clear lack of interest in the politics of these small wars. Tellingly, *The British Army Review* only published two articles on counterinsurgency between 1989 and 2001, whilst coverage of apolitical manoeuvre warfare was 'legion'.[18] Nevertheless, the political dimension remained paramount to war. Major General Robin Brims, commander of British land forces during Op Telic I, forcefully states that it was the "political process rather than the imperatives of operations that dictated how the armed forces would be used by the Coalition in the campaign. The primacy of politics is likely to be a constant factor in the conflicts of the future".[19] How this played out in practice is explored below.

THE INVASION OF IRAQ

Britain's main contribution to the ground component of the US-led Operation Iraqi Freedom was the 1st Armoured (United Kingdom) Division, which was nested within the US' 1 US Marine Expeditionary Unit. Critically, policy was aligned with tactical requirements. Prior to the invasion: "Prime Minister Tony Blair found the time to spend half a day with his military chiefs talking through the options and listening to their concerns [...] the UK government had arrived at a clear policy for the invasion itself and the Ministry of Defence had developed a good strategy to implement it."[20]

Major General Robin Brims briefs members of the media during Op Telic 1.
Courtesy of *Soldier*/Crown copyright

"Major General Brims understood that his mission was to break the grip of Saddam Hussain's Ba'athist regime, without alienating the Iraqi people and minimising collateral damage to the economically vital oil infrastructure. Brims was crystal clear on the necessity of linking his formation's plan to the overall US led effort, rather than being commanded from Northwood."

Major General Brims, general officer commanding 1 UK Division, therefore understood that his mission was to break the grip of Saddam Hussain's Ba'athist regime, without alienating the Iraqi people and minimising collateral damage to the economically vital oil infrastructure.[21] Brims was crystal clear on the necessity of linking his formation's plan to the overall US-led effort, rather than being commanded from Northwood. Consequently, his general officer commanding's directive stated that: "We are TaCom CG I MEF [coalition commander]. We create tactical effects to enable decisive delivery of his plans. We are integrating with HQ I MEF and its subordinate formations [...] We must also establish all our personal and electronic connectivities and processes with HQ I MEF. Our force is designed to be supported by I MEF deep assets."[22]

The campaign began on the night of 20th March 2003, when Royal Marines from 40 and 42 Commando landed by helicopter on the al-Faw Peninsula, tasked with securing the oil terminals in the area which were considered essential for promoting economic growth once a new government was established in Baghdad. The Marines, ably supported by British, US and Polish Special Operations Forces and the US Air Force, were able to rapidly secure these initial objectives and prevent the Ba'athist regime from sabotaging the facilities.[23] As the rest of the division crossed into Iraq from Kuwait and pushed north, Major General Brims noted that what: "Saddam wanted was for Coalition forces to enter cities such as Basra where the Iraqi forces could then try to force a Stalingrad or a Grozny-style battle. This type of urban battle would become a media event because of its awfulness, especially the civilian casualties. The international community might then be persuaded to demand a halt to hostilities and some form of ceasefire."[24]

Although the influence of the 'Manoeuvrist Approach' was apparent (Brims had declared as much in his general officer commanding's directive), the method was entirely appropriate for the campaign but critically made use of other approaches when the division reached Basra. Positional warfare was utilised by raiding Basra, using the heavy forces found in the 7th Armoured Brigade, which enabled sniper pairs to infiltrate and remain, denying parts of the city to the defenders. The most serious fighting came not from the Iraqi Army but irregular, broadly decentralised, Fedayeen

[16] *Freedman, Strategy, 202.*

[17] *Strachan, Direction of War, 19.*

[18] *Alderson, The Validity Of British Army Counterinsurgency Doctrine After the War in Iraq 2003-2009, (Cranfield University, 2009), 33.*

[19] *Brims, Operation Telic and the British Army in the Iraq Campaign of 2003, Australian Army Journal, Volume III, Number 1, 96-7.*

[20] *Elliot, High Command: British Military Leadership in the Iraq and Afghanistan Wars (Hurst Publishers, 2015), 151.*

[21] *Brims, Operation Telic.*

[22] *Reynolds, Basrah, Baghdad, and Beyond: U.S. Marine Corps in the Second Iraq War (Naval Institute Press, 2005), 123-4. This was partly because the British Army recognised that they were embedding into an American led plan and due to the time pressure to get the division ready for the proposed invasion date.*

[23] *Rossiter, Target Basra (Corgi, 2009); Kilcullen, Out of the Mountains: The Coming Age of the Urban Guerrilla (Oxford University Press, 2013), 276-8.*

[24] *Brims, Operation Telic.*

fighters. These clusters of resistance were defeated by attriting them in large numbers, rather than through a bold strike against an imagined centre of gravity. Throughout, Brims and his brigade commanders were able to bridge the gap between the policy goals and the ways and means available to them, without resort to an intermediary, apolitical level in between. The coalition's most optimistic expectations were realised when local Basrawis started to provide intelligence that allowed the coalition to target senior members of the Ba'ath party, dislodging them from the city which was liberated by 6th April.[25]

Critically, this is not to underestimate the level of operational artistry required to generate the tactical output that created strategic effect. The successful integration of air and naval gunfire companies from the 15th Marine Expeditionary Unit into 1 UK Division was achieved despite the condensed planning timeline leading up to the invasion.[26] Close coordination with a Marine Tactical Air Wing for deep fires, in lieu of the division's organic multi-launch rocket systems, was also highly impressive and essential given the logistical burden and likely collateral damage that would have been caused by the latter.[27] Information gathered from local human sources was fused with intelligence gathered from reconnaissance by Special Force detachments and from aerial surveillance by uncrewed aerial systems, that led to accurate strikes against Ba'athist strongholds.[28]

"The command relationship was further complicated by the fact that the British commander of Multi-National Division South-East also answered to Permanent Joint Headquarters, which began to exert tighter control on the campaign after 2003. This arrangement violated the principle of unity of command and distorted the ability of strategy to cohere tactics and policy."

This overview of the invasion has suggested that the operational level, as institutionalised in the form of Permanent Joint Headquarters, did not unduly distort the relationship between tactics and strategy during the invasion campaign. Most importantly, strategy appropriately cohered tactical action to achieve the desired political outcomes.

OPERATION SINBAD

After the invasion, the British remained in Basra and added command of the other three southern provinces to form Multi-National Division South-East. In theory the British commander directly answered to the American-led theatre command, Multi-National Force Iraq in Baghdad.[29] However, this clear chain of command had broken down by 2006 and the supposedly tactical boundary had evolved into a political divide, with the majority Shia south seen as a strategic backwater by US commanders whose main effort was in Baghdad and Anbar province where the Sunni insurgency was raging.[30] The command relationship was further complicated by the fact that the British commander of Multi-National Division

[25] *Murray and Scales, The Iraq War: A Military History (Belknap Press, 2005), 148; Urban, Task Force Black: The Explosive True Story of the SAS and the Secret War in Iraq (Abacus, 2012), 12; Reynolds, Baghdad, Basra and Beyond, 128-9.*

[26] *Reynolds, Basra, Baghdad and Beyond, 124.*

[27] *Brims, Operation Telic, 96.*

[28] *Murray and Scales, The Iraq War, 149-50. From a command perspective, the performance of the division and brigade HQs reached the high levels demanded of them, despite some measured and fair criticism, see Storr, The Command Of British Land Forces In Iraq, March To May 2003, Directorate General of Development and Doctrine – British Army, dodccrp.org/events/9th_ICCRTS/CD/papers/068.pdf*

[29] *This occurred because policy was being formed at the MoD, before being passed to PJHQ who then transmitted orders to the theatre commander. As noted, GOC MND-SE also answered to MNF-I, as well as dealing with constraints placed on his actions by Prime Minister al-Maliki who had his own agenda. When the same situation later manifested in Afghanistan, reporting lines were described as 'clear and neat as twigs in a bird's nest', quoted in Ledwidge, Losing Small Wars: British Military Failure in Iraq and Afghanistan (Yale University Press, 2011), 71.*

[30] *Maciejewski, "Best Effort': Operation Sinbad and the Iraq Campaign', in Blair's Wars, 158.*

A soldier from the 1st Battalion, Duke of Wellington's Regiment directs traffic at a vehicle check point in southern Iraq.
Courtesy of *Soldier*/Crown copyright

South-East also answered to Permanent Joint Headquarters, which began to exert tighter control on the campaign after 2003. This arrangement violated the principle of unity of command and distorted the ability of strategy to cohere tactics and policy, although the British were not alone in this regard.[31]

After three years of steadily declining security in the south, Major General Richard Shirreff took command of Multi-National Division South-East from July 2006 until January 2007. Shirreff was "perhaps the first general officer commanding genuinely to view his position as a tactical subordinate to his US corps commander as more important than his subordination to Permanent Joint Headquarters". He was also clearly unhappy with the attitude of the latter. He told his subordinate commanders that the "time has come to take the offensive against the enemy and challenge the defeatists who seem to pervade Whitehall [MoD] and much of Northwood".[32]

Lieutenant General Nick Houghton, then Chief of Joint Operations, the three-star lead within Permanent Joint Headquarters, consequently described the situation (possibly with a hint of understatement) as "a little tense".[33] Although Shirreff later acknowledged Permanent Joint Headquarters' role in helping in obtaining critical facilitators, including a counter-battery fire capability, there was reportedly more obstruction than support for his methods.[34]

Aside from the personality clashes, there was a more fundamental conceptual problem created by the lack of an interface between commander and strategist, or what Eliot Cohen has described as the "unequal dialogue", which requires policymakers to question, probe and challenge their military subordinates to ensure that they were achieving their given political aims.[35] In this case, strategy was unable to square tactical reality with policy aspirations because Permanent Joint Headquarters, as the operational level inserted between theatre command and policy "coped less well with the complexity and nuance of the counter-insurgency that followed [the invasion], not least because they were just too remote from the day-to-day events" and because "[Chief of Joint Operations] had no chance to understand or influence complex local circumstances, since he visited the operational theatre only once a month or less".[36]

From the outset, British counterinsurgency efforts in Iraq therefore failed to reach the ideal of Gray's strategy 'bridge' which links political aims and tactics, nor was operational artistry able to make up for the shortfalls of a failing political campaign, due to the underlying failure of the British to gain a sufficient understanding of the human terrain in Basra.[37]

Shirreff's intent for Operation Salamanca was to redeem the situation in Basra by defeating the militias, including the Jaish al-Mahdi and Iranian-backed 'Special Groups', that now dominated the city. Ultimately however, Shirreff's plan was hampered by the shift in Permanent Joint Headquarters' main effort to Afghanistan. This second campaign prevented the British from massing sufficient forces to clear Basra of the militias. Even when the theatre reserve was committed, force densities were shockingly low and the failure to properly train, house or equip the Iraqi Security Forces meant that the newly formed 10th Division of the Iraqi Army could barely muster two full battalions to support the operation.[38] Consequently, the objectives were scaled down and re-branded under the name of Operation Sinbad.

Despite the lack of resource, Sinbad aimed 'to be an exemplar of the new British cross-government doctrine for stability operations known as the Comprehensive Approach' which combined military action with civilian-led reconstruction efforts to promote stability.[39] Although initial security, battlegroup level, 'pulses' obtained short-term results, there was insufficient follow-up forces – either British, Iraqi or civilian – to hold and rebuild cleared areas. Accordingly, the insurgents simply waited for the campaign to move on before reappearing and violence within Basra increased after the operation concluded.[40] Significant progress was not made until 2008 when the 'Charge of the Knights' operation, led by the US and Iraqi government, achieved much of what Sinbad had attempted.[41]

CONCLUSION

Ultimately, Sinbad was a policy failure that was preordained when the Government chose to deploy 16 Air Assault Brigade to Helmand in the spring of 2006. Nonetheless, lessons regarding the utility of the operational level can be drawn from the two cases discussed above. The evidence suggests that maintaining a schism between tactical commanders and policymakers with an intervening operational level, will likely impede future operations. When Permanent Joint Headquarters was kept in the background during the invasion, Major General Brims was able to link tactics to a clearly articulated set of political aims and operational art was able to underpin a successful campaign. When the operational level distorted political understanding of the insurgency to policymakers, strategic performance was hamstrung.

After completing a review of strategic and operational command in both Iraq and Afghanistan, retired Major General Christopher Elliot argued that the British "political/military interface must be reformed so that the principal leaders are always physically co-located in theatre – it must never be entertained that they could be separated, with the ideal being an empowered, vice-regal duopoly of military and political persons".[42] This would go some way to achieving Gray's vision of bridging policy and tactics and Cohen's ideal of dialogue between politician and commander. Co-locating would also allow operational art to directly underpin effective tactical action rather than being conducted in separate conceptual and geographic spheres.

Lieutenant General Sir John Kiszely concludes his article on the operational level by arguing that the failure to take the concept seriously has "led some people towards the false logic that every tactical victory would lead to strategic success, and that, therefore, every opportunity to destroy the enemy should automatically be taken – what today might be termed 'the kinetic solution".[43]

---

[31] *Strachan quotes an exchange between Paul Bremer, head of the Coalition Provisional Authority, who stated 'that his job was policy and General Ricardo Sanchez's [Commander Multi-National Force Iraq (MNF-I)] was the war, and that each should stick to his own sphere. So, he should not have been surprised when he, not unreasonably, asked Sanchez for details of his tactical plans, and Sanchez responded, "Stop right there, sir. I am not going to give you the details of our tactical plan." Strachan, Direction of War, 20.*

[32] *Maciejewski, "Best Effort', 162.*

[33] *Ibid.*

[34] *Alderson, The Validity Of British Army Counterinsurgency Doctrine, 154-5.*

[35] *Cohen, Supreme Command: Soldiers, Statesmen, and Leadership in Wartime (Anchor Books, 2003).*

[36] *Elliott, High Command, 177, 176.*

[37] *For a critique of the coalition's approach to understanding the cultural and political milieux of Iraq see Tripodi, The Unknown Enemy: Counterinsurgency and the Illusion of Control (Cambridge University Press, 2021), 138-64.*

[38] *Maciejewski, 'Best Effort', 165.*

[39] *Ibid., 158.*

[40] *The significant number of anti-government militiamen in the police was a significant factor in the inability to consolidate gains. Maciejewski, 'Best Effort', 168.*

[41] *For an overview of this operation, see Iron, Basra 2008: Operation Charge of the Knights, in Blair's Wars.*

[42] *Elliott, High Command, 223.*

[43] *Kiszely, Thinking About the Operational Level, 42.*

Yet this is the very role that should be played by strategy, and it is perhaps this distorted view of the concept that led Brigadier Ben Barry to criticise the "tendency in the militaries of both the US and the UK to assume that achieving political effects was the responsibility of politicians".[44]

This was clearly demonstrated by Major General Jonathan Shaw, Shirreff's successor, who lamented that "it fell to me to take on responsibility for generating the strategic plan" – although Gray's (and Clausewitz's) theory would task the general with exactly this mission, on condition that clear policy objectives had been set.[45] Thus, hampered by the logic of an intervening operational level between tactics and strategy, Multi-National Division South-East failed to translate military power into sustainable political effect in Basra, a situation which ended with the British pulling out of Iraq in 2009.

[44] *Barry, Blood, Metal and Dust: How Victory Turned into Defeat in Afghanistan and Iraq (Osprey Publishing, 2020), 41.*

[45] *Quoted in Elliot, High Command, 124.*

Courtesy of *Soldier*/Crown copyright

AUTHOR

Major Robb Bloomfield (Army Cadet Force) is a full-time cyber security professional and part-time PhD student at the University of Buckingham.

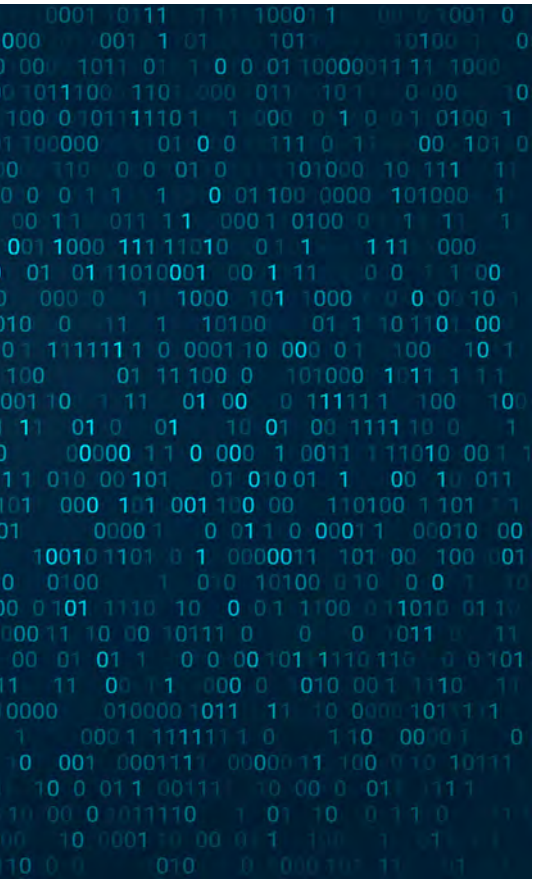
DIGITAL DIPLOMATS: THE CONCEPT OF CYBER PEACEKEEPING

THOSE in uniform have often found themselves at the vanguard of innovation, with conflict serving as an accelerant for the development of cutting-edge technologies. Thermal imaging, radar and LCD screens all carry the fingerprints of British military scientists and there can be no denying that operations in Iraq and Afghanistan expedited the evolution of unmanned air systems.

Defence does not, however, always find itself ahead of the curve and that is certainly true in the digital domain. The Internet as we recognise it turned 40 this year and yet cyberspace has only been formally recognised as a British national security matter since 2009.[1] And it wasn't until 2016 that NATO acknowledged cyberspace as the fifth formal domain of warfare. Consequently, as with the rise of air power a century ago, we may be on the cusp of a new paradigm of warfighting but are discovering rapid technological developments to be at odds with doctrine, legislation, and the nature of conflict as we know it.

The notion of whether war could be waged in cyberspace has been debated at length, and clear answers are not yet forthcoming. When considering the employment of information communication technologies for this purpose, it is clear that the Clausewitizian definition of war as an 'act of violence' is not met. References to 'armed attacks' in Article 2(4) of the UN Charter are also in opposition with the way we perceive our use of information spaces and only applies to states. The modern concept of 'new war' describes a loss of state control on the monopoly of violence, with a power transfer to criminal elements and cyber crime. The rise of non-state actors, private military contractors, and indeed the ability for anyone with access to a computer to

[1] *Cabinet Office, The National Security Strategy of the United Kingdom: security for the next generation, (London: The Stationary Office, 2009), p. 13.*



become a participant in a conflict introduces additional complications. But while these debates continue, cyber-attacks are being employed as a component of modern conflicts, and harm is being caused to civilians by the indiscriminate targeting of critical national infrastructures – 'the interconnected systems vital for society, health and welfare'.[2] By exploiting the ongoing normative uncertainty, attacks continue under the threshold of a formal response, and out of the reach of international humanitarian law. The malicious use of cyberspace therefore undermines global peace and security. The greatest wars of our time ushered in the formation of the United Nations, charged with keeping peace in an increasingly volatile world. While kinetic conflicts continue, peacekeepers have been engaged in 72 of them. The writers of the UN Charter couldn't predict the future, and if cyber-enabled warfare does become a reality, it would be wise that we should be prepared. In our modern, interconnected world, there is no agreed peace to keep, and citizens operate daily in an environment that is inherently hostile. On that basis, should peacekeeping be brought to cyberspace?

CONCEPT

The concept of cyber peacekeeping was first proposed by Cahill et al in 2003, with further researchers proposing expansions and potential frameworks.[3] Much of the work remains theoretical, as no mission has yet had

"In our modern, interconnected world, there is no agreed peace to keep, and citizens operate daily in an environment that is inherently hostile. On that basis, should peacekeeping be brought to cyberspace?"

to carry any such functions out. Analyses also focus on the assumption that consent has been obtained from belligerents – while this is one of the three core principles of peacekeeping, the invasive nature of accessing sensitive networks is almost certainly going to be denied. This may require the application of a mandate by coercive means, such as the modern concept of 'robust peacekeeping' or peace enforcement. The UN Capstone Doctrine defines 11 discrete peacekeeping activities, which can be divided into traditional, multidimensional and supporting role activities.[4] In considering how peace will be established in cyberspace, it will be necessary to map these activities to the digital domain. It is also necessary to establish the extent of the research area – cyberspace is described as having physical, virtual and cognitive dimensions,[5] and the tasks assigned to cyber peacekeepers would therefore need to encompass all three aspects.

TRADITIONAL ACTIVITIES

The core activities of traditional peacekeeping are ceasefire supervision; observation, monitoring and reporting; and the establishment of buffer zones. These activities are intended to be temporary, and to create stabilising conditions that will facilitate negotiations for a permanent end to a conflict. There is a degree of overlap to the processes, and feasibility themes are shared.

To have the intended effect and ensure adherence by the parties, the phrasing of a ceasefire agreement needs to be precise, without room for ambiguity. The constant evolution of capabilities undermines this requirement, along with the lack of international agreement on terms such as 'critical infrastructure', and the industry sectors concerned. The concept of geography also needs relating to cyberspace as agreements will typically include the boundaries and area of operation in scope. This could be a network definition, such as an autonomous system and all associated prefixes, but the usefulness of this approach is limited due to the distinct differences between a physical and logical network. Furthermore, once private networks are brought into consideration the area of responsibility could scale exponentially – even globally due to the significant amounts of infrastructure in private operation, potentially by entities which are headquartered in yet another third-party state. This global scaling also has implication for control of forces due to the ease with which proxies can be employed, along with the risk of external spoilers. As an example, the distributed denial of service attack against Estonia in 2007 may have originated from up to 178 different countries. The attribution problem is well known and, without reliable identification, attacks can happen with impunity.

The monitoring of operational computer systems is not a novel undertaking, however, gaining access, particularly in non-consent scenarios remains a significant barrier. One of the first tasks for any observation, monitoring and reporting regime would be to establish a baseline – it is critical to ascertain whether the observed platform is in a clean state, and what the initial parameters are. It is also important to establish what 'normal' activity looks like, particularly regarding network traffic patterns. Any changes detected can therefore be measured against the original model and accurately reported. Of course, the monitoring process captures far more information than just that concerned with potential military activity, which means the principles of neutrality and impartiality are critical for this activity, and peacekeeping activities will need to be carried out in a strict ethical and transparent framework. The physical dimension of cyberspace has relevance here as well, as the addition of new equipment to a network could indicate acquisition of specific capabilities, such as deep packet inspection equipment or network jamming – these may also indicate violations of sanctions. While encryption is vital for privacy and security of end users, it also aids those that would seek to conceal activity. Peacekeepers could also be required to monitor the availability of communications infrastructure to the public, rather than the conflict in isolation.

---

[2] *Cabinet Office, National Cyber Security Strategy 2016 – 2021, (London: The Stationary Office, 2016), p. 22.*

[3] *See, inter alia, Michael Robinson and others, 'An Introduction to Cyber Peacekeeping', Journal of Network and Computer Applications, 114, (2018), 70-87.*

[4] *United Nations Peacekeeping Operations: Principles and Guidelines, (New York: Department of Peacekeeping Operations, 2008), p. 19.*

[5] *Ministry of Defence, Cyber Primer, 3rd edn, (London: Development, Concepts and Doctrine Centre), p. 7.*

To assist with identification and verification processes, agreements may specify zones or cantonment areas to aid in directing troop movements. Buffer zones are used to create neutral areas absent of any military activity and could conceivably be employed to protect civilian infrastructures from cyber attacks. The restricted zone is used to prohibit a specific practice, such as use of aircraft or artillery. In virtual terms this could be used to forbid the employment of specific forms of cyber attack. Coordinated zones require troop movements to be planned with peacekeepers. A potential comparison could be a permissive window where tools and capabilities are transmitted over a network, perhaps as part of a disarmament or disclosure process. This could also apply to transmission of dual-use capabilities to aid transparency and further confidence building measures. But as shown, given that personnel engaged in a cyber-specific engagement can be geographically dispersed and anonymous, and detached from the systems they are using, it makes the process of implementing a defined zone of control significantly more difficult – or even impossible beyond the smallest of scales.

MULTI-DIMENSIONAL ACTIVITIES

Multi-dimensional activities involve a union of military and civilian formations, and for cyber peacekeeping that is likely to be expected at all levels due to the considerable technical expertise required from personnel. The focus now is on activities that either aid in moving to a post-conflict state, or which seek to maintain it, with an end-goal of maintaining stability with progression towards long-term recovery and development. Activities are now chiefly intrastate rather than involving all parties to a conflict and unlike the traditional peacekeeping activities there is significantly less overlap, which reduces constraints and potentially allows for more discrete application or one or more activity independently. The defined processes are disarmament, demobilisation and reintegration; mine action, human rights protection and promotion; electoral assistance; restoration and extension of state authority; and security sector reform.

The primary challenge to effective cyber-based disarmament, demobilisation and reintegration is defining 'weapons' and 'combatants'. Digital attack methods are non-tangible and, unlike conventional single-use munitions which irreparably distort or fragment when employed, can be replicated freely,

"As logic bombs represent clear staging for further attacks, their use could invoke the concept of imminent threat in international law, which justifies pre-emptive self-defence."

employed less discriminately and used ad infinitum. The focus cannot be on the means, but rather the impact or consequence. Code is a communication to a system to carry out an action, the effect of that communication can vary significantly, and therefore it may be impossible to restrict capabilities. It's also impossible to verify capabilities by count or by storage as they could be put on thumb drives and hidden, or even printed and filed. There is a high likelihood that those engaging in cyber attacks during a conflict are non-state actors, who may or may not be state sanctioned – the volunteer IT Army of Ukraine is a pertinent example. Demobilising such individuals may have to be a matter for the host state, and a further challenge would be ensuring that the resources to aid reintegration were received by the right people.

A common comparison for mine action in cyberspace is equating anti-personnel mines to conditionally executed malware or 'logic bombs'. In the electronic sense, software waits for a predetermined activity to occur, such as the system clock reaching a certain date, and then the payload is triggered. This type of attack is often associated with insider threats and there are numerous instances of personnel in positions of privileged access utilising them for the purposes of fraud. Like their physical counterparts, electronic 'mines' are problematic because they can remain effective long after conflict has ended if not triggered or removed. As logic bombs represent clear staging for further attacks, their use could invoke the concept of imminent threat in international law, which justifies pre-emptive self-defence. On this basis, they would be a priority for mitigation to prevent the return of conflict. While the analogy has some value, the environmental hazards of mines such as access denial, threats to biodiversity and chemical contamination are not usefully mapped to the realm of cyberspace and therefore the comparison is only used tangentially. The caution here is that analogies need to be employed carefully; when dealing with novel developments it may be that prior methods need to be discarded entirely.

In 2018 the United Nations' Human Rights Council affirmed 'that the same rights that people have offline must also be protected online',[6] giving cyber peacekeepers a clear role for human rights protection and promotion. The Council particularly referenced freedom of expression, as provided for in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Access to the Internet has been discussed as part of other activities, but additional considerations could be protection against discrimination, promotion of equal opportunities, and freedom of association and privacy. One of the biggest barriers to protecting citizens is the private nature of infrastructure and platforms, and providers being bound by domestic legislation – such as when Apple removed the Quran Majeed app

[6] *United Nations General Assembly, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', A/HRC/38/L.10, undocs.org/en/A/HRC/38/L.10 [accessed 03/2023]*

from the Chinese app store on the grounds it was hosting 'illegal religious texts'.[7] This also links to the concept of sovereignty, and how cultural attitudes differ. The imposition of specific values on a nation state during post-conflict disorder is certain to fail without long-term application and stability and may be at odds with concepts of neutrality and impartiality.

The right to participate in free and fair elections is a fundamental human right, which is discharged by democratic conduct of the same. The will of the people in choosing political representation without interference is also a foundation of national sovereignty. Contributions to the UN Open-Ended Working Group and Group of Government Experts fora highlighted the threat of digital election interference. Durable norms are required not just for infrastructure but also for processes. Recent allegations of election interference have focused on the use of influence operations, such as in the 2016 US presidential election where Russian actors engaged in substantial campaigns to proselytise the candidacy of Donald Trump. Duties of peacekeepers could consist of detecting and responding to false information or providing cyber security functions to digital aspects and mitigating attacks on infrastructure. A complication arises when states engage in internal manipulation to maintain power, and matters of sovereignty apply once again.

Where exceptional circumstances require it, the Security Council may authorise peacekeepers to assume legislative and administrative functions of a state on a temporary basis, either to provide structures that were lacking or assist with the transfer of authority. Restoration and extension of state authority is therefore concerned with stabilisation and may be of most relevance for states with a low cyber dependence in the form of capacity building.

Security sector reform is the process of reconstituting the state institutions that provide for safety and security, such as law enforcement and institutions responsible for civil emergencies. It complements disarmament, demobilisation and reintegration and aims to transfer former combatants into long-term employment in the security sector. This could include development of a national cyber security strategy, provision of technical support and logistical assistance. In transferring skills to national personnel there must be a proviso that the training would enable a return to civil society, and recipients must not be able to leverage the knowledge gained to initiate further conflict. In a post-conflict environment, training could

"Recent allegations of election interference have focused on the use of influence operations, such as in the 2016 US presidential election where Russian actors engaged in substantial campaigns to proselytise the candidacy of Donald Trump."

Image by freepik.com

also be provided for cyber crime prosecution, such as in the case of the Global Prosecutors E-Network. There is a continuing risk that as technical experts are in short supply, solutions may be implemented that reflect their own national models absent the cultural factors of the present operation.

SUPPORTING ROLE ACTIVITIES

Supporting role activities are concerned with aiding UN civilian agencies and partner non-governmental organisations to maintain a lasting peace and providing established multi-dimensional missions with additional taskings. Peacekeepers could therefore find themselves providing a cyber defence capability to these agencies, who may not have the skills to provide their own. The principle of last resort from the *Oslo Guidelines* has relevance for these activities – 'foreign military and civil defence assets should be requested only where there is no comparable civilian alternative'.[8] This is where various stakeholders in global infrastructure, such as the Internet Corporation for Assigned Names and Numbers and the regional internet registries, could play a larger part in ensuring their functions promote a peaceful agenda.

Due to the nature of humanitarian assistance and disaster relief functions, tasks cannot be fully planned for and preparation is therefore based on 'most likely' scenarios, with deployment at short-notice and for variable length periods. The availability of suitably trained personnel may therefore be a barrier. Many conflicts have commenced with the cutting of telecommunications cables, such as the two World Wars, the Korean War and Gulf War. The nature of assistance could therefore include restoring communication services or provision of cellular access to ensure that citizens have access to information. During the 2022 escalation of the Russo-Ukrainian war, security company Cloudflare declared that Russia 'needs more Internet access, not less' in recognition of this point, however, this resulted in them being targeted by the 'Internet Troops of Ukraine' in retaliation. This raises the ongoing security of peacekeeping missions as an additional factor for consideration.

When transitioning from a situation of conflict to long-term peace, there must be efforts to assist socio-economic recovery and development. This would consist of capacity building initiatives to develop polices, institutions, human resources and skills so that states can fully engage with a digital world. Many state functions are increasingly moving online, such as taxation and legal transactions, and assistance could be provided in establishing these utilities and services. Long-term resilience is the end-goal for peacekeeping; it needs to be accepted that cyberspace will likely remain hostile and therefore weathering and recovering from attacks is what should ultimately be focused on.

CONCLUSIONS

Currently, there are numerous feasibility issues that would prevent cyber peacekeeping from becoming established. Key themes have emerged from the cursory examination, such as legal, technical and operational barriers. The practical use of this concept is therefore currently low – beyond anything other than the smallest scales, however, the need for progress and the prevention of harm remains and as the nature of conflict continues to evolve future examinations should look to alternative, non-traditional measures which would be useful in establishing peace where cyber-enabled conflict has occurred.

Sir Hugh Trenchard, first Marshal of the Royal Air Force, warned of 'the rude awakening'[9] that would befall those that did not consider the fledgling realm of air as a primary medium of war; as we look to the future of warfare and the role that cyberspace will play in those conflicts, can we avoid our own?

---

[7] *BBC, 'Apple Takes Down Quran App in China', (2021), bbc.co.uk/news/technology-58921230 [accessed 03/2023].*

[8] *Office for the Coordination of Humanitarian Affairs, 'Oslo Guidelines: Guidelines on the Use of Foreign Military and Civil Defence Assets in Disaster Relief', (2007), unocha.org/sites/unocha/files/OSLO%20Guidelines%20Rev%201.1%20-%20Nov%2007.pdf [accessed 03/2023], p. 8.*

[9] *David Ian Hall, 'The Long Gestation and Difficult Birth of the 2nd Tactical Air Force (RAF)', RAF Air Power Review, 5.3, (2002), 20-31 (p 25).*

DIGITAL DISPATCHES: INSIDE THE RANKS OF UKRAINE'S IT ARMY

AUTHOR

Andrew Simms is editor of *The British Army Review* and – during a 12-year tenure working for the Ministry of Defence – reported extensively from Kosovo, Iraq and Afghanistan.

"My name is Harv Xavier. I spent a significant portion of the 1990s and 2000s chronicling malware development. I consider myself a pentester [penetration tester], forensic investigator, state-sponsored hacker and ***one of the most prominent hacktivists within the IT Army of Ukraine****."*

MY INTERVIEWEE is not your traditional soldier. He has no military training, command experience or direct link to the flag he fights for. And yet my questions are answered from Ukrainian soil[1] by a volunteer very much embroiled in the war raging on Europe's eastern borders. As a senior figure in the IT Army of Ukraine, which was created in the immediate wake of Russia's invasion at the behest of Mykhailo Fedorov, Ukraine's Minister of Digital Transformation and First Vice Prime Minister, Xavier's arsenal is equally unconventional – spearheaded with a keyboard and mouse rather than any form of kinetic weaponry.

Fighting in the digital domain as opposed to the trench systems found on the physical frontlines has not, however, denied the Harvard-honed hacker from amassing his share of 'war stories'. Since answering the cyber call to arms last year, the computer scientist has – with the "cooperation of comrades" – brought traffic in Moscow to a standstill by hailing hundreds of taxis through an app owned by tech giant Yandex, 'Russia's Google'; stolen and made public the personal data of mercenaries contracted to the Wagner Group; and launched a "sweeping attack" on Russia's largest internet service provider that took the country's banking system offline.

"The Ukrainian IT Army is a threat actor comprised of international and Ukrainian

[1] *The author of this article has no reason to doubt the authenticity of the responses provided. However, given the need for anonymity, it is not possible to verify if the answers shared are solely his own or accurately reflect the official stance or operations of the IT Army.*

hackers working in collaboration with officials from Ukraine's Ministry of Defence to target Russian infrastructure and websites," explained Xavier. "Over 15 months, more than 700 targets have been attacked. The Russians do not know where the attacks are coming from – we sneak behind their networks and infrastructure security tracks astutely. The IT Army has suspended the work of a bunch of Russian sites and online resources, including military stores and stores of drones and radio equipment. We have made a series of DDoS [distributed denial-of-service] attacks on specialised stores so that newly mobilised Russians cannot purchase quality equipment."

Xavier's contribution to the IT Army of Ukraine's extensive taskings, which relate to defending against digital intrusion of Ukrainian information and cyberspace as well as the conduct of offensive cyberwarfare operations, began by invitation. He was approached by a member of The International Legion of Territorial Defence of Ukraine with links to a major US defence company and asked to assist in protecting critical infrastructure from cyber attacks, but he says his decision to 'join up' was driven by a desire not to be a passive bystander to a bloody conflict.

"The IT Army has suspended the work of a bunch of Russian sites and online resources, including military stores and stores of drones and radio equipment."

He told *The British Army Review*: "Four Russian presumptions have been proven to be incorrect since the start of the conflict on the 24th February, 2022: that the Ukrainian Government would fall and Russian forces would quickly seize Kyiv and other Ukrainian cities; that the European Union would struggle to demonstrate resolve and respond to this aggression; that the 'Western world' would be divided and uncertain in its reaction; and that the larger international community would not denounce Russia's invasion. I kept reading the news and just thought that I had the skills to come over here and help in some manner.

"I cannot deny that I am working for the IT Army, but at the same time I refuse the idea of having been recruited for the Ukrainian Army. Yes, I was invited internationally to volunteer by military institutions and civil firms because of my experience in the field of information technology, pentesting and media strategy, but I and many of my comrades are trying to fight evil and save what can be saved for a better future and a world free of conflicts."

With no military-style training establishments in the field of hacking to shape standards and drill tactics, techniques and procedures, Xavier described as diverse the skill sets and backgrounds of his plentiful peers.

"The IT Army has gathered more than

230,000 anonymous volunteers who are working together to fight on the cyber front," he said. "Believe it or not, a lot of hackers are self-taught. Others go to college to learn cyber security, some are academics and many of them are experts working for various intelligence services. Everything you learn about cyber security can be used to bypass cyber security."

The group's strength and trust in 'faceless' numbers, use of gamified scoreboards to recognise top performers and heavy reliance on social media platforms, such as Telegram and X (formerly Twitter), for communicating sets it far apart from conventional military organisations. Its set up and unusual modus operandi also suggest a distinct lack of command and control. The opposite is, however, true.

"We operate in a beehive," Xavier said. "There are about 1,000 people working within the IT Army and we, as moderators, discuss and organise work internally when it is presented to us by the official in charge of each sector. We then distribute tasks to the rest of the team according to priorities, specialisations and the legitimacy of response, and based on the importance of the message and inevitability of results. IT Army leaders foster productive working relationships, lessen conflict and support the accomplishment of missions through developing trust with peers, superiors and subordinates.

"Both offensive and defensive cyber units are formed from the voluntary recruits. The defensive squad is used to defend infrastructure like power plants and water systems, while the offensive volunteer unit aids Ukraine's military by conducting digital espionage operations against invading Russian forces. The IT Army of Ukraine and its cyber warriors have daily target lists that we share with other friends on the dark web."

These targets are not necessarily synchronised with ground operations.

"Coordination of operations between conventional and cyber forces is challenging," argued Xavier. "First, there is a problem with conflicting goals. Intelligence-oriented actors prefer covert long-term access to a system over short-term system disruptions, which are more likely to reveal the used backdoor and thereby exhaust the capability. Second, the physical locations of digital and conventional battlefields rarely align."

However, the IT Army does not work in isolation and enjoys close ties with industry and government.

"A lot of hackers are self-taught. Others go to college to learn cyber security, some are academics and many of them are experts working for various intelligence services. Everything you learn about cyber security can be used to bypass cyber security."

"Many major tech companies, such as Google and Amazon Web Services, have stepped up to help support Ukraine with their respective specialities – a decision their executives claimed to be simple. A company based in London that is a leader in the field of UAV systems and IT engineering has helped us a lot in reducing the potential impacts of drone-based cyberattacks, which can range from data theft and disruption of services to physical damage.

"The government of Ukraine is drafting a new law to bring its volunteer hacker brigade into the armed forces. It supports us a lot, but conditionally. Ukraine's National Coordination Centre for Cybersecurity recently suggested the IT Army should become the basis for developing the state's cyber defence capabilities, enlisting cyber volunteers and establishing a cyber reserve – a group of civilian cyber experts who have received military training and who could be mobilised to assist in the defence of the country during times of increased cyber threat."

Formally incorporating the IT Army into the Armed Forces of Ukraine would put an end to uncertainty about its status in a legal grey area that has drawn pointed warnings from the Red Cross for attacking civilian targets such as Russian banks, food delivery services and video-sharing sites. But Xavier is clear in his mind that no moral lines have been overstepped.

"What you realise when war comes to a country is that there are no good ways or bad ways to protect something," he continued. "The IT Army has served as an example for other nations. Several other countries have reserve military units with cyber capabilities, but if the law is passed, Ukraine would join a handful of other Western countries, led by Finland and Estonia, that have a full-scale reserve cyber army to supplement their regular military and maintain, process and troubleshoot military systems and operations. This, I think, will be the beginning of working towards achieving faster attacks than seen in conventional wars or [a capability that can] hold back enemy forces.

"In my opinion, Ukrainian hackers have demonstrated in the first year of the full-scale war that, despite the invasion, they behave ethically enough and do not significantly harm any subjects save those of Russia that are engaged in the conflict.

"Attacks on civilians are prohibited by the Geneva Convention, a set of principles designed to lessen the brutality of physical wars. However, the Geneva Convention does not apply to cyberwarfare. According to the International Committee of the Red Cross, current codes should be followed. Therefore, attacking hospitals, for example, would be a breach and is what Russian hackers do when they lose their dignity. They go far to attack innocent people, we do not."

While Xavier's contribution to the Ukrainian war effort does not demand close proximity to Russian rifles, computer firewalls can't shield against missiles and, as history tells us, those who poke Putin's administration often face severe retribution. Xavier says his comrades are conscious that digital missions can lead to physical repercussions but that the risk of harm does not diminish their resolve to see Russia defeated.

"If you live in a conflict zone, your goals are far more urgent than they are for those who are fortunate enough to not do so. Simply remaining alive and making it to the next day is your primary objective. It's possible that you spend much of your time setting emergency goals, which are a lot of modest, short-term objectives that are essential for preserving personal safety, food and shelter. This also means that you are improving your ability to determine the finest details of a target plan because you constantly have to determine the tasks required to get by each day.

"The Kremlin lists the IT Army among the top four active hacking groups defending Ukraine alongside Squad303, American Ghostclan

and Georgian GNG. We may be targets on the Russian intelligence 'FSB' hit list in the future, but it does not mean that the IT Army is being monitored. This is impossible as we are invisible – even our beloved families don't know much about our cyberwarfare operations against the 'Orcs'.

"We are watching them closely and our attacks will be increased against them day after day until victory. In the first quarter of this year, the volume of DDoS attacks in Russia increased by 58 per cent compared to last year. The geography of attacks has also expanded and although they have become less likely to lead to 'unacceptable events' for targets, the low cost of hackers allows us to continue to use the tactics of 'carpet bombing' a wide range of companies and institutions."

As a content creator and media strategist, Xavier has also been at the forefront of providing the IT Army of Ukraine with an authoritative voice in a heavily congested and contested mire of messaging from Ukrainian, Russian and international sources. Making high-quality content that "locks in belief" and "drives business" has been pivotal to preserving a mass of willing cyber warriors and is supporting Ukraine's wartime strategic communications, according to our anonymous source.

"There are innumerable images of the war in the media, both traditional and social and this is a significant test of the Ukrainian people's defensive spirit, so anything that preserves the nation's spirit and highlights that there is still hope for them to emerge from this dark period is beneficial.

"I believe that information operations emphasise the bad images of 'them' while propaganda emphasises the good images of 'us'. To influence, disrupt or usurp the decision-making of potential adversaries, the Russians always turn to information operations during military operations. Ukrainians love to hear propaganda – they react to news of a thorough attack on an Orc factory like they have just won the lottery. The impact of the attack on the ground is near miraculous.

"The deliberate confusing and undermining of information environments are Russian tactics. Their actions aim to create ambiguity, impede attempts at consensus-building, and increase support for Russia's objections while weakening the legitimacy of Ukraine's response. Undermining the information space to achieve this goal has negative repercussions for all democracies, however, it poses the greatest risk in fragile democracies grappling with complicated historical, sociological and economic difficulties, such as Ukraine.

"To address the challenges to democracy and freedom of expression, it is essential to comprehend how the Russian government controls domestic media environments as well as how misinformation is disseminated overseas. To introduce, enhance and distribute false and distorted narratives around the world, Russian actors use a variety of tactics and strategies. It uses a variety of fake and artificial identities and accounts, anonymous websites and official state media sources to disseminate and amplify contents that serve its objectives and discredits opposing viewpoints.

"I am sure that Russian propaganda and disinformation campaigns are created in massive quantities and disseminated through a variety of online and offline means. Paid internet 'trolls', or individuals who post provocative, deceptive statements via online chat rooms, discussion forums and comment sections on news and other websites, are among the creators and distributors of this content. In fact, Russia is attempting to control the majority of the national television networks, radio stations, media markets and newspapers, either directly or through friendly business magnates and state-owned companies."

Penetrating such a wall of Russian noise represents a formidable task and is likely to prove as difficult as the military struggle to liberate Ukraine. Xavier may not be your average soldier, but like those combatants attempting to break through Russia's heavily fortified defensive lines, he is adamant that the will to win is greater amongst Ukraine's ranks and will ultimately be the decisive difference.

"I am always alert to upcoming danger as I am facing a mean enemy, but I still trust that victory belongs to those who believe in it the most and believe in it the longest."

CYBER COUNSEL FROM A CYBER CONFLICT

When asked about how best to shield from cyber attacks, Harv Xavier offered *British Army Review* readers the following tips:

Monitoring for credential misuse is very important. If you want to carry on working throughout a conflict, you should be prepared for communications to be unstable and have backup plans for how to communicate via alternative means. When cooperating with counterparts in Ukraine, organisations and individuals take extra effort to monitor, inspect, and isolate traffic from those organisations and individuals and to assess the access controls for that traffic.

Russian APTs [advanced persistent threats], such as Gamaredon, use strategies that are comparable to those of other highly successful outfits. Their techniques, tactics and procedures are not kept a secret. It's also important to note that many of the cyber attacks recorded in Ukraine have included computers to which the attackers appear to have had prior access. Preventing these dangers demands paying attention to the basics of security. Although it was intended for Ukrainian firms, the disk-wiping malware application HermeticWiper affected several contractor locations in the neighbourhood.

> "Cyber attacks are viewed as a viable option by Orcs to deter adversaries, control escalation and resolve disputes."

Organisations with no connection to the region are more likely to fall prey to independent threat actors located in Russia that want to hurt NATO and Ukraine's friends abroad – those seen as adversaries of the Russian government.

IT [personnel] should minimise changes and inspect all new software, newly-created accounts and high privilege accounts. In addition, the need for strong authentication is increasing, especially for privileged accounts, and change control and monitoring should be enhanced. Improve basic health and safety, even if only temporarily.

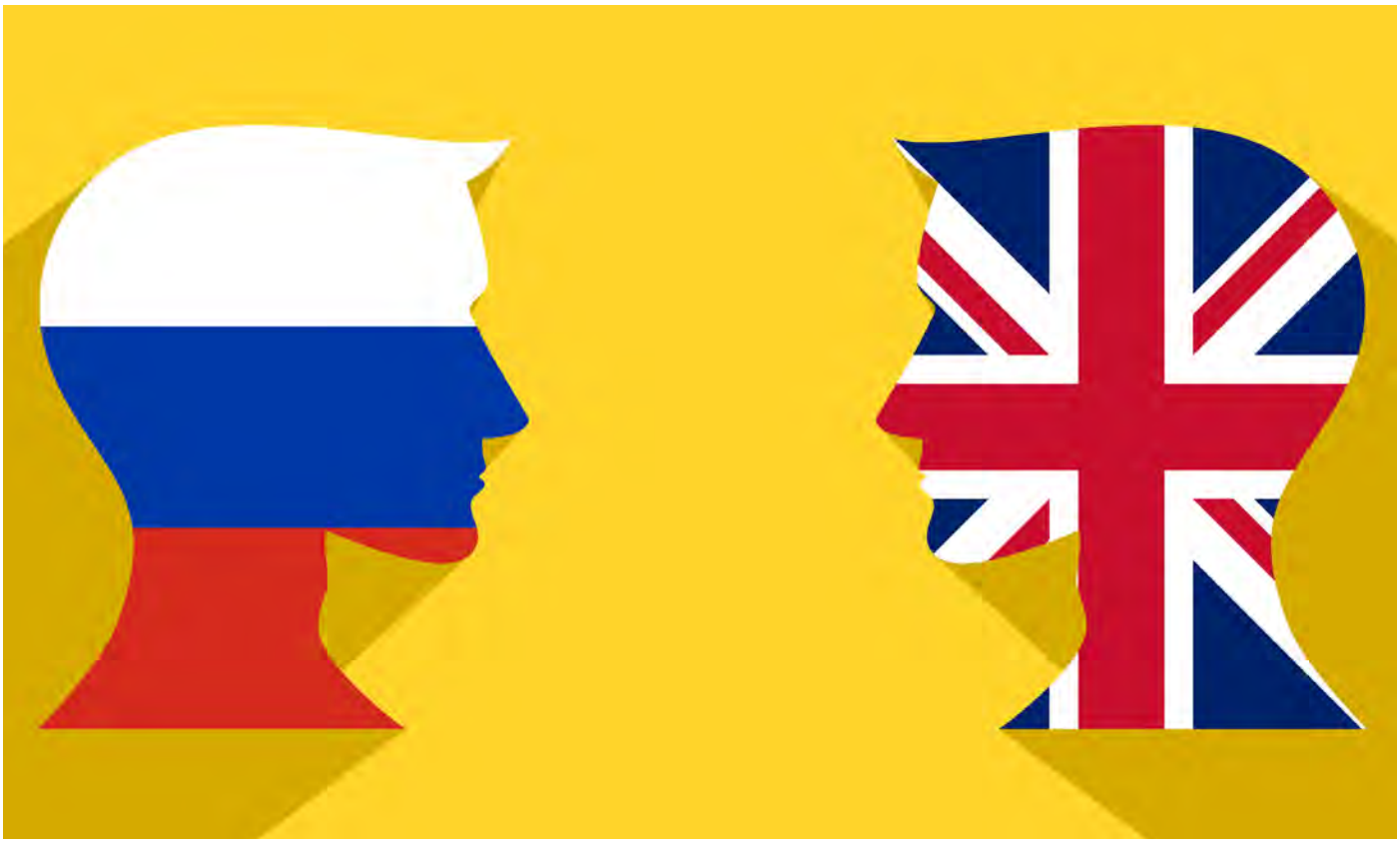
Employing search resources like Censys and Shodan, organisations and individuals should review their security posture by checking for exposed network boundaries and demilitarised zones.

Monitor outbound traffic for signs of malware targeting command and control sites from your network. Nation-state malware usually needs to communicate in some way, but can be very difficult to detect.

Disable legacy authentication.

Remind everyone in your organisation that people are the most likely target of an attack.

Security teams should reassess senior-level connections and communications on politically sensitive issues, including social media posts criticising Russia. Consider launching an insider playbook to address potential security issues from malicious insiders.



FACING UP TO RUSSIA'S ACTIONS: DOES THE UK NEED TO REAPPRAISE ITS PREVIOUS STRATEGIC ASSUMPTIONS?

AUTHOR

This article was penned by **Major Simon Swindells** and assessed to be among the top essays submitted by officers on the January-July 2023 intake of the Intermediate Command and Staff Course (Land). *The British Army Review*, in liaison with Defence Academy directing staff, will publish further articles by Joint Services Command and Staff College students in future editions.

THE Global Britain strategic narrative – the centrepiece of the UK's capstone strategy issued in 2021, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy* – is the result of a determined effort by the Government to establish an ambitious role for the country following its departure from the European Union. Whilst acknowledging the ever-present Russian threat, it argues that the world's geopolitical and economic centre of gravity will move eastwards towards the Indo-Pacific,[1] with China becoming a leading global power. The *Integrated Review* states that this requires a realignment in the UK's approach to shape and take advantage of these changing dynamics.

This article defines 'strategic assumptions' as those statements set out in the *Integrated Review's* strategic framework. It argues that the expansive aims fail to appropriately centre the UK's posture in the Euro-Atlantic region against an endemically belligerent Russia, which risks a loss of credibility with allies and foes alike. Whilst doing so will limit the broad-horizon approach of Global Britain, especially the much-vaunted Indo-Pacific tilt, the UK should focus its security posture within the Euro-Atlantic whilst concurrently developing wider political and trade links. This will reinforce the UK as the pre-eminent security partner to the US, European states and other allies and better protect its core interests.

DRIVERS OF GLOBAL BRITAIN

Global Britain seeks to enunciate the UK's approach as an independent state outside the European Union; it is "the latest attempt to answer Dean Acheson's famous challenge: for Britain to find a suitable role for itself in the World".[2] The political drivers of the policy are beyond this article's focus, but this essay agrees with the premise that a combination of economic and population growth and China's increasing assertiveness mean that "for the

[1] *United Kingdom. Cabinet Office. Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy. (London, 2021): 26.*

[2] *Sir John Sawers, "The Integrated Review: Innovative Thinking But Still Some Blind Spots," The Integrated Review in Context (2021): 23.*

UK to be a global player it has to accept that [the] Indo-Pacific is the new geopolitical centre".[3] Further, the policy accords with the Government's determination to characterise "Brexit as a unique opportunity to rethink its foreign and security policy: stronger, more influential, more global".[4]

The nature of recent British engagement in the Indo-Pacific, such as the 2021 Carrier Strike Group deployment and AUKUS pact, the enhanced UK-Japan Reciprocal Access Agreement, along with trade deals with Japan, Australia, New Zealand and the UK's application to join the Comprehensive and Progressive Trans-Pacific Partnership, gives a clear indication of its approach. Whilst further trade links are welcome, the war in Ukraine demands "a careful calculation of where resources can best be utilised in support of British national interests".[5] From a military perspective, the UK's aspirational core assumption that it can remain deeply invested in European security whilst also projecting permanent force postures beyond existing levels in the Indo-Pacific requires reconsideration.

REAPPRAISING ASPIRATIONS SINCE RUSSIA'S INVASION OF UKRAINE

When considered against the *Integrated Review*'s strategic assumptions, the impact of Russia's invasion of Ukraine on the UK's foreign policy is profound. The UK's ambitions do not adequately answer the realistic security challenges it faces, which the *Review* itself outlines: the Euro-Atlantic region will remain critical to the UK's security and prosperity; Russia will remain the most acute direct threat to the UK; and the US will continue to ask its allies in Europe to do more to share the burden of collective security.[6] Russia's invasion has revealed with alarming clarity the extent to which it will pursue its agenda, and is "an inflection point for European and global security".[7] Further, the Kremlin's mindset demonstrates a zero-sum sense of besiegement and isolation which makes further belligerent action likely.[8]

> **"Russia's appetite for violence – threatened or real – to coerce its smaller neighbours and to maintain its status means that 'regional security and stability will be elusive', and clear-eyed choices on strategic prioritisation are required."**

The war in Ukraine forces the UK to confront the inherent tension between its global aspirations and the changed realities of Europe's security picture. This long-standing tension results in the criticism that "the UK thus faces the prospect of trying to do too many things and not doing any of them well".[9] As the Chief of the General Staff noted in his speech announcing a refocussing of the Army under the codename Op Mobilise, "Russia will be an even greater threat to European security after Ukraine than it was before".[10] The proposition that the UK was able to commit a significant proportion of its foreign policy instruments – including its military – to engagement and constraint operations throughout the world now looks imprudent. Within the *Integrated Review*: "Nowhere is there a recognition that resources – whether of people, budgets or ministerial energies – are finite. In the end, good strategy comes down to making choices."[11] Russia's appetite for violence – threatened or real – to coerce its smaller neighbours and to maintain its status means that "regional security and stability will be elusive",[12] and clear-eyed choices on strategic prioritisation are required. "Global Britain is characterised by a reluctance to make choices and has added commitments which it is neither equipped nor resourced to meet."[13]

This desire to forge an exciting new role for the UK has led to a downplaying – in tone, if not explicitly – of the threat from Russia. The 2022 NATO Strategic Concept, which states that "the Russian Federation is the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic area",[14] as well as the 2022 US National Security Strategy, which states that "Russia now poses an immediate and persistent threat to international peace and stability",[15] provide clear guidance as to where the UK must readjust its focus. An aspiration to project extensively beyond the Euro-Atlantic is not the role that the UK should be fulfilling in NATO or within the US-UK relationship. "The term 'tilt' implies a tilt away from something; in other words, away from Europe towards the Indo-Pacific. This is not the message the UK should be sending to the world."[16] Rather, the UK's response since the Russian invasion provides an excellent template for an impactful future strategic role.

A more realistic approach of being the leading partner in containing Russian aggression and reassuring allies in the Euro-Atlantic area, particularly in the Baltic and Black Sea regions, will also reassure the US and "free up US assets to do their stuff on our behalf in the Indo-Pacific... that is a more coherent strategy that plays to our strengths".[17] The significant redeployment of US assets in Europe in response to Russia's belligerence will have wider implications for the US's ability to out-compete China, adding greater impetus to the need for the UK to refocus its attention closer to home. The UK should continue to develop its force posture and engagement in the contentious areas of the Euro-Atlantic, in order "to prevent the Kremlin from again seizing the initiative and writing the future unimpeded".[18] The recent security pacts between the UK, Sweden and Finland,[19] the UK's role as Framework Nation in the Joint Expeditionary

---

[3] *Patrick Wintour, "Why Britain is tilting to the Indo-Pacific region," The Guardian, March 15 (2021).*

[4] *Claudia Major and Nicolai von Ondarza, "No "Global Britain" after Brexit," SWP Comment, no 24 (2018): 1.*

[5] *Anisa Heritage and Pak K. Lee, "'Global Britain': The UK in the Indo-Pacific," The Diplomat (2021): thediplomat.com/2021/01/global-britain-the-uk-in-the-indo-pacific/ (accessed January 31, 2023).*

[6] *UK, Integrated Review, 26.*

[7] *Ed Arnold, "The Case Against Reviewing The Integrated Review," RUSI Commentary (2022): rusi.org/explore-our-research/publications/commentary/case-against-reviewing-integrated-review (accessed January 25, 2023).*

[8] *Dr Maxine David and Dr Natasha Kuhrt, "The Consequence of Foreign Policy: The Review and Russia," Centre for Defence Studies series on The Integrated Review in Context: A Strategy Fit for the 2020s? (2021): 74.*

[9] *Peter Magill and Wyn Rees, "UK Defence Policy After Ukraine: Revisiting the Integrated Review," Survival 64, no 3, (2022): 95.*

[10] *Gen Sir Patrick Sanders, Speech at the RUSI Land Warfare Conference, 28 Jun 22, gov.uk/government/speeches/chief-the-general-staff-speech-at-rusi-land-warfare-conference*

[11] *Lord Peter Ricketts, "The Integrated Review in Context: The Importance of Hard Choices," The Integrated Review in Context, (2021): 14.*

[12] *Robert Dalsjö, Michael Jonsson and Johan Norberg, "A Brutal Examination: Russian Military Capability in Light of the Ukraine War," Survival 64, no. 3 (2022): 22.*

[13] *Hew Strachan, "Global Britain in a competitive age: Strategy and the Integrated Review," Journal of the British Academy, 9 (2021): 161.*

[14] *NATO. Strategic Concept 2022. (2022): 4.*

[15] *United States of America. The White House. National Security Strategy 2022. (Washington, 2022): 25.*

[16] *House of Commons Foreign Affairs Committee, "Refreshing our approach? Updating the Integrated Review" Fifth Report of Session 2022-23, (18 December 2022), 18.*

[17] *General Richards, Baron Richards of Herstmonceux, in conversation with Dr Philip Berry, youtube.com/watch?v=Hc9XIyKp7aU (accessed January 31, 2023).*

[18] *Dr Alexander Lanoszka and James Rogers, "'Global Britain' and the Black Sea region," Council on Geostrategy (2022): 30.*

[19] *United Kingdom. Prime Minister's Office. (London, 2022): gov.uk/government/news/prime-minister-signs-new-assurances-to-bolster-european-security-11-may-2022 (accessed February 2, 2023).*

Leading role: Under Op Interflex, the UK is continuing to train personnel from the Armed Forces of Ukraine
Courtesy of *Soldier Magazine*, © Crown copyright

"Leveraging the UK's pre-eminence in support for Ukraine, as well as the shared determination of European countries to confront Russian aggression, is an excellent building block to rebuild UK-EU relations."

Force,[20] its strategic framework and dialogue with Greece and Germany respectively, as well as its participation in the Northern Group forum, offer a strong base of evidence to further reinforce the UK's commitment to Euro-Atlantic security. An increase in the scale and frequency of British military commitments in the Baltic and Black Sea regions, with a particular focus on working within NATO as well as with other partners such as the EU, will ensure that the UK "sustain[s] its role as a convener of the broader liberal democratic community",[21] that it has so effectively demonstrated since February 2022. Continuing to build closer trade and political links in the Indo-Pacific, whilst tilting the UK's military efforts back towards Europe, is a much more balanced and secure long-term strategy.

POSITIVE IMPLICATIONS FOR UK-EU RELATIONS

The UK's departure from the European Union, the ongoing dispute about the Northern Ireland Protocol, as well as the paucity of security considerations in the EU-UK Trade and Cooperation Agreement 2020, have all had negative impacts on UK-EU relationships. Nevertheless, "this Brexit hangover is damaging to both parties, especially in a world where European countries, whether in or out of the EU, have shared values as liberal democracies and those values are coming under severe challenge".[22] Russia's invasion enables the UK to reposition itself as the key security partner in the Euro-Atlantic to the US and European nations. Resolving issues relating to the Northern Ireland Protocol, and developing a closer EU-UK security partnership, are two such initiatives that will further strengthen Euro-Atlantic security. Ultimately, "at some point, [the UK] needs to recognise that if Europe is insecure, the UK will also be insecure".[23] The March 2022 EU Strategic Compass for Security and Defence, and the deepening of NATO-EU security ties via the January 2023 Joint Declaration on EU-NATO Cooperation, offer an impetus for the UK Government to build a more mutually beneficial relationship with its European partners. Leveraging the UK's pre-eminence in support for Ukraine, as well as the shared determination of European countries to confront Russian aggression, is an excellent building block to rebuild UK-EU relations.[24]

CONCLUSION

Russia's invasion of Ukraine has focussed and unified the UK and its allies commendably, but has also highlighted the *Integrated Review's* inherent flaws. The UK's overambitious Global Britain strategy, especially its focus on the Indo-Pacific, is not grounded in the updated reality of the enhanced, long-term Russian threat to Europe. The UK Government must seize the opportunity to reappraise its strategic assumptions to provide more clarity and realism; its interests are not served by "a refreshed document that is based on empty rhetoric or overly ambitious posturing".[25] It must recentre the UK's focus on maintaining Euro-Atlantic security alongside its desire to pursue greater Indo-Pacific engagement, which will strengthen relationships with the US and European partners and make the UK a more effective, adroit security actor in its key alliances.

---

[20] *United Kingdom. Ministry of Defence. (London, 2022); gov.uk/government/publications/joint-expeditionary-force-policy-direction-july-2021/joint-expeditionary-force-jef-policy-direction (accessed February 2, 2023).*

[21] *Sir Robin Niblett, "Global Britain in a divided world," Chatham House (2022): 40.*

[22] *Sawers, "Integrated Review," 24.*

[23] *Ian Bond, "Can the UK be secure if Europe is not? The UK's (un)integrated review," Centre for European Reform Insight (2021): 3.*

[24] *Niblett, "Global Britain," 3.*

[25] *HoC Foreign Affairs Committee, "Updating the Integrated Review," 4-5.*

Published by Quercus, Paperback, £12.99, ISBN-13: 9781529427813

TITLE
My Russia: War or Peace?

AUTHOR
Mikhail Shishkin

REVIEWER
Captain Rob Weale, RGR

A WINDOW ON RUSSIA'S 'SLAVE-MASTER' SOCIETY

In this surprising book, the multiple prize-winning Russian author and dissident Mikhail Shishkin explains the violent, gangster-ridden political economy of modern Russia by contextualising it in over a thousand years of history.

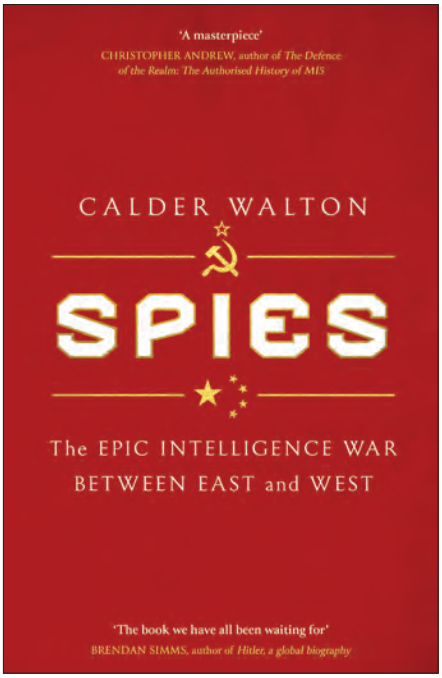
Shishkin's family history is typical of his generation. His grandfather was "disappeared" by the Secret Police in the 1930s, his uncle executed in a prisoner of war camp by the Nazis, and his father dead of alcoholism in the "chaos" of the 1990s. His assessment of politics is unavoidably affected by this tragic hinterland; he casts the Russian people as mentally "enslaved" and suggests that they are unsuited to democracy. Shishkin was brought up behind the Iron Curtain and makes consistent references to Cold War-era Russians' utopian conception of Western Europe, which he stands in contrast to the miserable, pseudo-European society of Russia. Rather than the Viking founders of the Kyivan Rus, much beloved by Putin, Shishkin claims that the real origins of Russian politics lie in the medieval Mongol conquest of Muscovy.

The author represents the Russian state as the court of a modern "Great Khan", with elements of *The Godfather*–style gangsterism thrown in. Complex webs of patronage and ruthless power-politics determine the Russian game of thrones. Shishkin draws a thread through Mongol, Tsarist, Soviet and "democratic" rule to argue that Russians have a fundamentally different attitude than Europeans to power and the state. Shishkin prizes Enlightenment values, particularly liberty, but he considers Russian cultural icons who share this, such as Pushkin and Rachmaninov, as a separate caste from the ordinary Russians. What separates these "European Russians" from the descendants of the serfs is the belief that individuals have value and should be respected as more than merely another commodity at the whim of the state. Their rarity is the point: these giants are exceptional because most Russians are not like them. Most Russians, historical and modern, are depicted as a peasant mass, resigned to their exploitation by the powerful and fearful of change.

"The author represents the Russian state as the court of a modern 'Great Khan', with elements of *The Godfather*–style gangsterism thrown in. Complex webs of patronage and ruthless power-politics determine the Russian game of thrones."

One of the primary lessons of Russian history is that no situation is so awful that it cannot be rendered even worse. Shishkin's analysis of Russia's class system reveals that venal and incompetent leadership has deliberately prevented the emergence of a bourgeoisie to entrench its own position, and that consequently there is nothing between the massed peasantry and the extractive, avaricious aristocratic elite. This slave-master relationship, in contrast to the thriving middle classes of European democracies, has prevented the emergence of genuinely participatory politics. Shishkin draws no distinction between Tsarist and Soviet Russia here; although the aristocracy may have been formed of different individuals, their power relationship with the proletariat was the same.

This is a depressing read for those anxious about Russia's, and Europe's, future. The assertion that most Russians value "strong" leadership ahead of any other characteristics such as integrity or inspiration bodes poorly for an uncertain post-Putin landscape. Shishkin is superb in explaining the "otherness" of Russia, and why their quest to subjugate Ukraine defies military and political logic. This book is an essential primer for those looking to understand who Russians are as a means to explain why they act the way they do.



Published by Little, Brown Book Group, Hardback, £25, ISBN-13: 9781408714959

TITLE
Spies: The Epic Intelligence War Between East and West

AUTHOR
Calder Walton

REVIEWER
Captain Ben Tomlinson, Visiting Fellow, CHACR

SHEDDING LIGHT ON A SHADOWY WORLD

Exploring the murky world of KGB, CIA and MI5/6 operations since the Russian Revolution, *Spies* anchors itself in the analysis of Western and Soviet espionage, sabotage and subversion throughout this period. What sets Calder Walton's offering apart from other examinations of Cold War espionage, however, is the belief that an effective understanding of these events may present answers for contemporary frictions with China.

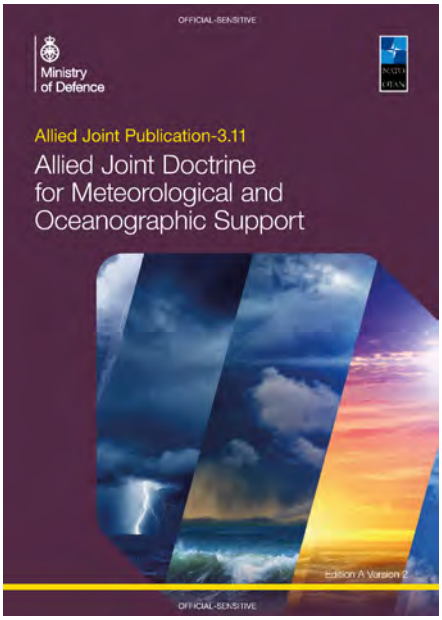
The author, a well-established commentator on intelligence and security, has previous form as the principal researcher for Christopher Andrew's tome *Defence of the Realm: The Authorised History of MI5*. Although he asserts that "intelligence attracts nut jobs, hacks and conspiracists like moths to a flame", *Spies* is far from the ramblings of a hack. Walton lays out his stall early and highlights several key assessments in the introductory chapter concerning the Cold War and the ongoing intelligence struggle with China. However, *Spies* is an extremely ambitious book. Seeking to cover a period of well over 100 years, whilst also exploring contemporary intelligence issues, it does fissure into two halves.

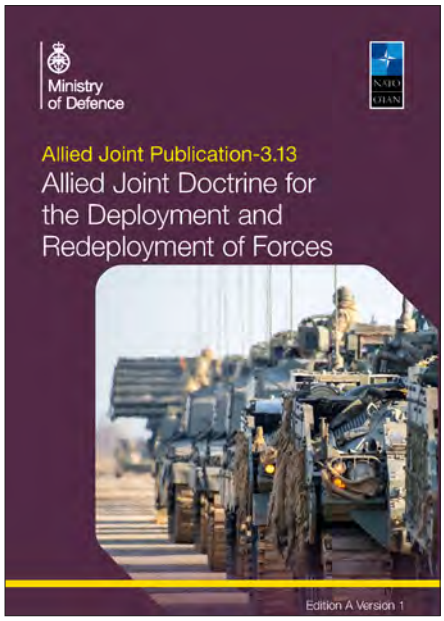
The first half is an historical examination of the competition that has existed between Western and Soviet intelligence agencies since their inception. This section, which makes up the lion's share of *Spies*, is fascinating and clearly supported by an inordinate amount of primary research. However, Walton's anecdotes concerning UK, US and Soviet intelligence do feel somewhat directionless until we are introduced to the second half of his work in the 18th, and final, chapter.

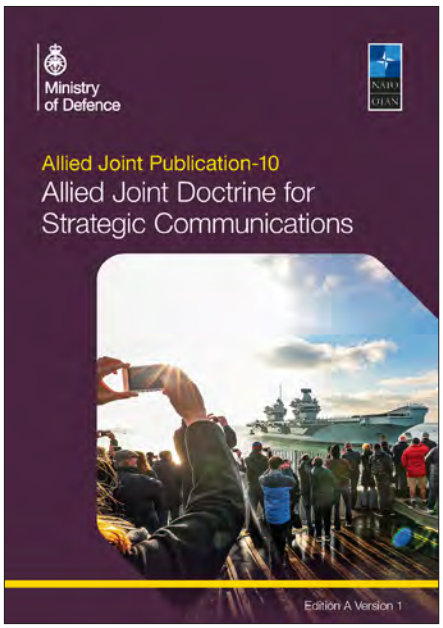
"Like Soviet intelligence during the last century," he writes, "Chinese agencies are waging a persistent, integrated, and asymmetric onslaught on Western countries." The West are particularly susceptible to a "whole of society" espionage approach which the Chinese Community Party readily employs. He adds that Chinese intelligence services, Chinese companies and Chinese nationals will overwhelm Western intelligence agencies and steal Western science and technology. As Walton concludes, "while last century's superpower contest was an arms race for nuclear superiority and computing, this century's context will involve a race for the control of data".

Overall, Walton's colloquial and conversational style makes *Spies* an enjoyable read. The author guides us through to his foretold conclusions without oversimplifying and makes compelling observations on impending intelligence competitions. However, *Spies* overextends itself without satisfyingly concluding either of its components. Walton acknowledges that this is not a comprehensive history of Cold War espionage but doesn't delve deep enough in the second half to justify the first. Nonetheless, an engaging book with some stark warnings.

DOCTRINE







The publications produced by the Development, Concepts and Doctrine Centre are to guide military operations and inform professional military education as personnel progress through their career.

Allied Joint Publication-3.11, *Allied Joint Doctrine for Meteorological and Oceanographic Support* provides guidance for planning, executing and assessing meteorological and oceanographic support throughout the full spectrum of NATO activities. The publication describes the contribution of meteorological and oceanographic support to the operational commander's situational awareness, risk management and environmental exploitation. It outlines NATO meteorological and oceanographic support capabilities, tasks and responsibilities. The doctrine provides guidance for joint NATO commanders and staff on how to use meteorological and oceanographic capabilities to support activities including operations. It also features guidance for subordinate commands and non-NATO entities participating in NATO activities that receive NATO meteorological and oceanographic support.

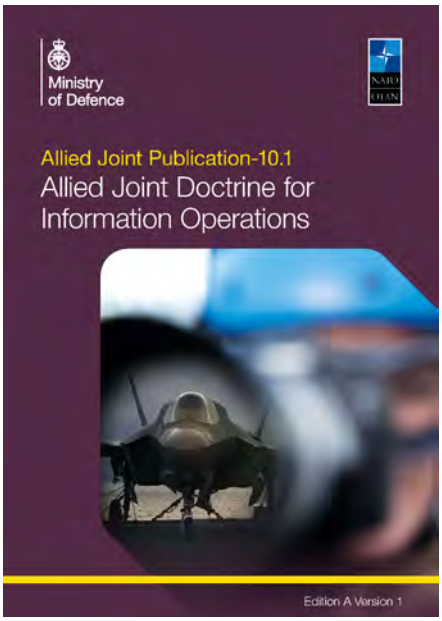
Allied Joint Publication-3.13, *Allied Joint Doctrine for the Deployment and Redeployment of Forces* articulates the common framework surrounding the command, coordination and synchronisation aspects of deployment and redeployment for Allied joint operations. It covers the fundamental principles and structures and systems and procedures required for effective deployment and redeployment of forces. The publication emphasises that deployment and redeployment are separate stages of an operation. They are delivered through the joint core activity, 'sustain', and are enabled through the joint function, 'sustainment'. This publication is intended primarily as guidance for commanders, staffs and forces at the joint operational level, but it is also a valuable reference for coalitions of NATO member states, partners, non-NATO nations and other organisations.

Allied Joint Publication-10, *Allied Joint Doctrine for Strategic Communications* with UK national elements is the keystone doctrine for Strategic Command and all information and communication related activities. This publication now includes UK-specific additional text to describe the UK context and organisation of Defence Strategic Command. It introduces Strategic Command as the primary function for ensuring all NATO activities are conceived, planned and executed with a clear understanding of the importance of informing and influencing the perception, attitudes and behaviours of audiences to achieve objectives. This publication supersedes *Joint Doctrine Note 2/19*. The publication is primarily for use by UK Defence and NATO commanders and their staff at the military-strategic and operational levels, but has equal relevance at other levels. It is also an important reference for Alliance and partner nations at all levels because it offers a framework for operations, missions and tasks conducted by a coalition of NATO partners, non-NATO nations and other organisations. It provides a reference for NATO and non-NATO actors.

Allied Joint Publication-10.1, Allied Joint Doctrine for Information Operations with UK national elements explains how Information Operations staff ensure coordination and synchronisation of information activities. It focuses on the operational level to support commanders' objectives and now includes UK-specific notation and examples to explain the UK organisation and employment of Information Operations, as well as offering operational examples of their application. Information Operations are applicable in peace, crisis and conflict throughout the continuum of competition. The publication provides a framework for conducting information environment assessment, audience analysis and planning activities for cognitive effect. It supersedes *Allied Joint Publication-3.10, Information Operations*. The publication provides guidance to UK Defence and NATO commanders and their staffs to use Information Operations as the staff function for the horizontal integration of strategic communications direction and guidance through planning and coordinating information activities throughout the full spectrum of activities and operations. It clarifies the role of Information Operations staff within the communication directorate, emphasising their responsibility for coherence and their key contribution to joint operations.

Doctrine publications and supporting documents can be found at the following links:

- Defnet – Development, Concepts and Doctrine Centre (**sharepoint.com**)
- DCDC App on the Defence Gateway Development, Concepts and Doctrine Centre (**mod.uk**)
- GOV.UK – Development, Concepts and Doctrine Centre (**gov.uk**)
- YouTube – Publications may be supported by introductory videos and audio books which can be accessed from the Development, Concepts and Doctrine Centre YouTube channel.



The Development, Concepts and Doctrine Centre Doctrine Team writes authoritative threat-informed NATO and UK strategic and operational level doctrine to inform professional military education and guide operations. By putting 'NATO at the heart of UK defence' it is able to achieve maximum coherence and interoperability with, and between, close allies and partners. Where possible, it will adopt NATO doctrine (Allied joint publications) rather than producing national doctrine (joint doctrine publications). Where it cannot, it will make sure that the UK remains compatible. UK specific 'best practice' is preserved through a small number of UK specific publications with supplementary elements added to NATO publications where required.

The Land Warfare Centre Warfare Branch published the following manuals, handbooks and doctrine notes during summer 2023.

Battlegroup Small Uncrewed Aircraft Systems Handbook, Edition 1

The increasing use of uncrewed aircraft systems, previously the preserve of specialist military units, represents a rapid development in capability across the battlefield. Adversaries, both state and non-state, alongside allies, partners and civilians, now have access to systems at a scale which has led to military commentators, think-tanks and organisations questioning whether their use represents a fundamental change in the character of conflict. This debate is ongoing, but the advantage provided to those who can effectively leverage the capability of uncrewed aircraft systems, either as a sensor or strike capability in support of tactical actions, has been categorically proven.

In recognition of the importance of uncrewed aircraft systems in contemporary operations, the Land Warfare Centre has developed this first edition of the *Battlegroup Small Uncrewed Aircraft Systems Handbook*. It provides guidance on planning and execution at the tactical level that will enable battlegroup staff to effectively integrate uncrewed aircraft systems. Moreover, this handbook provides a baseline for all uncrewed aircraft systems operators and commanders to understand their role within a battlegroup or sub-unit operation.

The *Battlegroup Small Uncrewed Aircraft Systems Handbook* is the Field Army guide to open and S1 classes of uncrewed aircraft systems. It should be read in conjunction with *Army Doctrine Publication Land Operations (2022)*, supports *Army Field Manual Conventional Warfare* and is essential reading for all small uncrewed aircraft systems users, as well as battlegroup commanders, their staff and sub-units wishing to become small uncrewed aircraft systems capable.

The Fundamentals of Combined Arms Manoeuvre, Edition 1

The Fundamentals of Combined Arms Manoeuvre references our capstone doctrine, complements the broader Army field manuals and draws on contemporary experiences of potential adversaries and allies. It is a distillation of numerous learned insights and experience from training, operations and war and offers commanding officers proven methods for success. The document is intended to be a start point for the expression of our thinking on combined arms manoeuvre fundamentals.

The publication describes the enduring core tenets of combined arms manoeuvre. It will continue to iterate as we adapt to the changing character of warfare and the tools available to us and our opponents such as small uncrewed aircraft systems, electronic warfare, cyber and electromagnetic activities and informational tools. This document does not seek to replace our doctrine and you will find nothing that does not already exist in it, rather you will find a clear articulation of the practice of our doctrine, so a synthesis of doctrine and experience.

The Fundamentals of Combined Arms Manoeuvre is primarily aimed at battlegroup commanders and below. Taking around 30 minutes to digest, it should be read by all and available in battle-boxes for exercises and operations for reference. It should also be used to aid conceptual development; commanders and their staff should analyse the advice within against their area of specialisation and develop mechanisms for how they will put it into practice. Finally, it should be studied in all arms groupings to understand how capabilities can be combined to deliver effects greater than the sum of their parts.

"THE PURPOSE OF THE BRITISH ARMY IS TO PROTECT THE UNITED KINGDOM BY BEING READY TO FIGHT AND WIN WARS ON LAND."

ARMY

CHACR

CHACR.ORG.UK