



Óglaigh
na hÉireann
IRISH DEFENCE FORCES

Defence Forces Review 2025



www.military.ie

DEFEND
OUR STATE



Óglaigh
na hÉireann
IRISH DEFENCE FORCES

Defence Forces Review 2025

DISCLAIMER

The material and views expressed in these papers are those of the authors, which have been subject to academic peer review, and do not indicate official approval of the Defence Forces or the Department of Defence.

ISSN 1649-7066

Published for the Military Authorities by
the Public Relations Section at the Chief of Staff's Branch,
and Printed at The Defence Forces Printing Press, Blackhorse Ave, Dublin 7.

© Copyright in accordance with Section 56 of the Copyright Act, 1963, Section 7 of the University of Limerick Act, 1989 and Section 6 of the Dublin University Act, 1989.

「 DEFEND
OUR STATE 」



The Command and Staff School

The Command and Staff School is the premier institution delivering professional military education for senior officers of the Irish Defence Forces. The school strives for excellence through higher learning, promoting an environment where critical thought and rational decision making is encouraged and developed. To this end, the Command and Staff School actively engages with government agencies, and academic institutions and militaries from around the world to ensure the prospectus remains fit for purpose in a volatile and uncertain contemporary operating environment. The main deliverable of the school is the Joint Command and Staff Course (JCSC), which Maynooth University accredit to Masters of Arts level. The JCSC prepares senior officers to transition from tactical level leadership to effective competence in command and staff appointments at the operational and strategic levels. The course achieves this by developing the students' intellect, analytical decision making, and communication skills. The JCSC can only be successful if the values, environment, ambience, and ethos of the Command and Staff School are conducive to learning, reflection, and personal development. To uphold and develop this philosophy, the school staff create and maintain a harmonious atmosphere, based on the highest professional military standards, that appeals to student's abilities, creativity, and imagination. The staff's role in editing the Defence Forces Review is testament to their professional character, academic competence, and commitment to highest standards of learning and education.

Launch of the Defence Forces Review

In conjunction with an Academic Seminar



Foreword

Building on the success of last year's Review, this year's theme is 'Military Leadership Challenges in the Contemporary Operating Environment.' This is a global issue of significant importance to Ireland and the Irish Defence Forces.

While the nature of armed conflict is enduring, it has a changing character, shaped by technological, economic, cultural, and societal changes. Ireland's security environment is characterised by increased contestation and volatility. The return of war to Europe, in addition to shifting global and political alignments, is challenging the Rules-Based International Order. Malign actors will continue to threaten our way of life using a variety of sophisticated means employed below the threshold of armed conflict.

The 2025 Defence Forces Review continues the tradition of past editions in providing a forum for intellectual debate within the wider Defence Community on matters of professional interest from which we can all learn.

My thanks to the editors of the Defence Forces Review 2025, Lt Col Gavin Egerton and Comdt Kenneth O'Rourke. Despite their very busy schedules in 2 Bde HQ and the Command and Staff School, they shouldered this editorial burden with energy, commitment, and enthusiasm.

For this year's edition, they have had the pleasure of working in academic collaboration with Dublin City University. A special word of gratitude to their fellow editors, Dr Eleanor Leah Williams and Dr Ken McDonagh, for their expert insights and invaluable contributions in making this collaborative effort a success. Many thanks also to Assoc Prof John McMackin for leading the collaborative effort and for helping to arrange the launch today.

I would also like to thank the staff of the Defence Forces Printing Press for the detailed and painstaking work they undertook in formatting the articles and designing the excellently presented Review you have received today.

Again, many thanks to all our contributors, without whose commitment and generosity the production and publication of this year's Review would not be possible.

Further copies of the Review are available from the Defence Forces Public Relations Branch at info@military.ie or online at <http://www.military.ie/info-centre/publications/defence-forces-review>.

James Sharkey
Lt Col
Officer in Charge
Public Relations Branch

Réamhrá

Ag cur leis an rath a bhí ar Athbhreithniú na bliana seo caite, is é téama na bliana seo ná ‘Dúshlán Cheannaireachta Míleata sa Timpeallacht Oibriúcháin Chomhaimseartha.’ Is saincheist dhomhanda í seo atá thar a bheith tábhachtach d’Éirinn agus d’Óglaigh na hÉireann.

Cé go bhfuil nádúr na coinbhleachta armtha buan, tá carachtar athraitheach aici, atá múnlaíthe ag athruithe teicneolaíocha, eacnamaíocha, cultúrtha agus sochaíocha. Tá timpeallacht slándála na hÉireann tréithithe ag méadú ar an iomaíocht agus ar an luaineacht. Tá fillleadh an chogaidh ar an Eoraip, chomh maith le hailínithe domhanda agus polaitiúla atá ag athrú, ag cur dúshlán roimh an Ord Idirnáisiúnta atá Bunaithe ar Rialacha. Leanfaidh gníomhaithe mailíseacha de bheith ag bagairt ar ár mbealach maireachtála ag baint úsáide as réimse modhanna sofaisticiúla a úsáidtear faoi bhunthairseach na coinbhleachta armtha.

Leanann Athbhreithniú Óglaigh na hÉireann 2025 traidisiún na n-eagrán roimhe seo maidir le fóram a sholáthar le haghaidh díospóireachta intleachtúla laistigh den Phobal Cosanta níos leithne ar chúrsaí gairmiúla ar féidir linn go léir foghlaim uathu.

Mo bhuíochas le heagarthóirí Athbhreithniú Óglaigh na hÉireann 2025, an Leifteanantchoirnéal Gavin Egerton agus an Ceannfort Kenneth O’Rourke. In ainneoin a sceidil an-ghnóthacha i gCeanncheathrú an 2ú Briogáide agus i Scoil an Cheannais agus na Foirne, ghlac siad leis an ualach eagarthóireachta seo le fuinneamh, le tiomantas agus le díograis.

I gcás eagrán na bliana seo, bhí an-áthas orthu oibriú i gcomhar acadúil le hOllscoil Chathair Bhaile Átha Cliath. Focal buíochais speisialta dá gcomh-eagarthóirí, an Dr Eleanor Leah Williams agus an Dr Ken McDonagh, as a léargais shaineolacha agus a gcuid ranníocaíochtaí luachmhara chun an iarracht chomhoibríoch seo a dhéanamh rathúil. Míle buíochas freisin leis an Ollamh Comhlach John McMackin as an iarracht chomhoibríoch a threorú agus as cabhrú leis an seoladh inniu a shocrú.

Ba mhaith liom buíochas a ghabháil freisin le foireann Chlóphlódóireachta Óglaigh na hÉireann as an obair mhionsonraithe agus chrua a rinne siad agus iad ag formáidiú na n-alt agus ag dearadh an Athbhreithnithe atá curtha i láthair go sármhaith atá faighte agaibh inniu.

Aris, buíochas mór lenár rannpháirtithe go léir, gan a dtiomantas agus a bhflaithiúlacht ní bheadh táirgeadh agus foilsiú Athbhreithniú na bliana seo indéanta.

Tá tuilleadh cóipeanna den Athbhreithniú ar fáil ó Bhrainse Caidreamh Poiblí Óglaigh na hÉireann ag info@military.ie nó ar líne ag <http://www.military.ie/info-centre/publications/defence-forces-review>.

James Sharkey
Leifteanantchoirnéal
Oifigeach i gCeannas
An Brainse Caidreamh Poiblí

Editors' Notes

The contemporary operating environment faced by militaries in 2025 remains in a state of constant evolution. While the full scale invasion of Ukraine by Russia in February 2022 brought territorial defence back to the fore, it did so as an additional layer on top of the evolving hybrid and grey-zone threats that face Ireland and the world. The contemporary operating environment requires an agility of mind and planning that is somewhat unprecedented. Both mass mobilisation and targeted technological innovations are required to meet the moment. Shadow fleet operations targeting subsea infrastructure, bot armies undermining social cohesion, and networks of funding and cooperation between hostile state actors and domestic organisations ranging from education to commercial activities to political subversives shape the contemporary strategic environment. Layered on top of this are a series of technological innovations that have transformed the battlefield. Increased computing power at lower cost and the commercial availability of what until recently would have been considered advanced drone technology have shifted the balance between cost and battlefield dominance. The drone incursions in Poland in September 2025 highlighted the asymmetry between unmanned aerial systems that cost thousands against airframes that require billions of euro to develop and maintain. The lesson here is that technological dominance in the battlefield is no longer necessarily a function of state investment but rather the challenge is in responding to and adapting to these shifts with agility and foresight.

This issue of the Defence Forces Review addresses these challenges head on, asking how the military leader needs to adapt and evolve to manage and overcome these contemporary operating challenges. It considers the role of leadership in responding to these immediate threats, but also its role in shaping conditions for organisational agility, resilience, and ethical decision making in these increasingly uncertain times. It engages critically with questions of how and when new technological solutions such as AI can be useful, while also not eschewing traditional leadership development training and techniques such as wargaming. Collectively, the papers in this Review demonstrate that the Defence Forces is already developing leaders and leadership skills capable of tackling these current challenges in an increasingly complex strategic landscape.

This Review also publishes abstracts from the research theses completed by Irish and international students from the 7th Joint Command and Staff Course, who completed an MA in Leadership, Management, and Defence Studies, taught in partnership between Maynooth University and the Command and Staff School in the Irish Military College. This partnership has developed over two decades and has seen hundreds of students from the DF graduate with master's degrees. Each year the Command and Staff School publish dozens of theses on defence related topics promoting professional military education in accordance with international best practice and helping frame and progress the Defence Forces' future in an ever uncertain and challenging defence environment.

The Defence Forces Review 2025 is published in collaboration with Dublin City University. The joint editorial team was Dr Ken McDonagh and Dr Eleanor Williams, Dublin City University; and Lieutenant Colonel Gavin Egerton and Commandant Kenneth O'Rourke from the Irish Army. The writing and production of this volume would not have been possible without the efforts of all who have contributed to it, including the authors, the (anonymous) peer reviewers, and the team from the Defence Forces Printing Press, especially Private Glenn Goulding. The editors would like to thank them all for their hard work.

Dr Ken McDonagh

Dr Eleanor Williams

Lieutenant Colonel Gavin Egerton

Commandant Kenneth O'Rourke

Editors' Biographical Statements

Dr Eleanor Leah Williams. Dr Williams is an Assistant Professor in Security at Dublin City University. Prior to joining DCU, Dr Williams held a Junior Research Fellowship with the Quill Project, at Pembroke College, University of Oxford. Here she advanced her research on the covert role of civil servants during the Northern Irish peace process. She has published on issues surrounding intelligence, negotiation, and security in journals such as *Critical Studies on Terrorism and Intelligence* and *National Security*.

Dr Ken McDonagh. Dr. McDonagh is Associate Professor of International Relations in the School of Law and Government at Dublin City University. His research is focused on EU Foreign Policy and Common Security and Defence Policy (CSDP), the role of small states in CSDP, Ireland's security and defence policy, and the gendered impact of CSDP missions. He has published on the EU as a global actor, the gendered impact of CSDP missions and contributed to policy papers and training activities in the area of Women, Peace, and Security and CSDP.

Lieutenant Colonel Gavin Egerton. Lt Col Egerton is an infantry officer with 23 years of service in the Irish Army. He commenced his career with 3rd Infantry Battalion, later serving in a variety of command, staff, and training appointments in infantry units, Defence Forces Headquarters, the Infantry School, and, more recently, the Command and Staff School. Lt Col Egerton has deployed overseas on operations on four occasions: once each with MINURCAT (Chad) and EUTM Mali; and twice with UNIFIL (Lebanon). He holds an MA with First Class Honours in Political Communication from Dublin City University, and he is currently completing a PhD at University College Cork, where his thesis title is *"The Application of Mission Command in Multinational Forces."* He is a member of the U.S. Army's Lieutenant General (ret) James M. Dubik Writing Fellows Program and has a keen interest in developing academic writing in the Irish Defence Forces. Lt Col Egerton is a graduate of the U.S. Army's Command and General Staff Officer Course. He is currently serving as Operations Officer, 2 Brigade Headquarters.

Commandant Kenneth O'Rourke. Comdt O'Rourke is an infantry officer with 23 years' service in the Irish Army. He has served in various command, training, and staff appointments, including Chief Instructor of the Infantry Weapons Wing, Infantry School; Officer Commanding 1st Mechanised Infantry Company; and as a staff officer in Strategic Planning Branch. He has served overseas with KFOR (Kosovo), UNIFIL (Lebanon), and as Deputy Commanding Officer of the Force Reserve Company in UNDOF (Golan Heights). Comdt O'Rourke completed a BA at the University of Galway and has completed a one-year exchange programme at the French Military Academy of St. Cyr. Comdt O'Rourke holds an MA in Teaching and Learning from South East Technical University, where his dissertation explored the practical application of educational wargaming in Professional Military Education (PME) to develop decision-making and planning skills. He is a recent graduate of the Joint Command and Staff Course and is currently serving as an instructor in the Command and Staff School.



Contents

Leadership without Location: Commanding the Contemporary Operating Environment Beyond the JOC Battalion Sergeant Major Shane McEneaney	1
How Can Coaching and Mentoring Support DF Personnel in Dealing with Redesigning and Transforming the Force in a Complex World? Corporal Yvonne Kearney, Brigadier General Brendan McGuinness	11
Military Leadership Challenges in the Contemporary Operating Environment. Educating the Modern Leader - Embracing Informal Learning in the Irish Defence Forces Corporal (AR) Fearghal Fitzgibbon	23
Simulating Complexity: Urban Operations, Cognitive Load, and the Role of Wargaming in the Contemporary Operating Environment Lieutenant Colonel Brian Cahill	33
From the Epoch of Total Lies to the Epoch of Total Distrust: Leadership Challenges and Doctrinal Shifts in Contemporary Hybrid Warfare Zurab Bezhanishvili	45
From Bayonets to Bits and Bytes: Leadership in the Information Environment Commandant Killian Doyle	55
Fog, Friction, Fragmentation: Military Decision-Making in an Age of Mosaic Warfare Commandant Simon Keenan	67
Maintaining Ethical Leadership in Grey Zone Operations Dr Dennis Vincent	77

Harnessing the Power of Story: Inoculating the Force against ‘Grey-Zone’ Effects Commandant Tadhg O’Donoghue	87
Bridging the Generational Gap: Leading Gen Z and Gen Alpha in the Post-Truth Era Sergeant Stephen McCabe	95
The Return of (Maritime) Hybrid Warfare As a Leadership Challenge for Europe’s Democracies Dr Brendan Flynn	105
Theses Abstracts 7th Joint Command and Staff Course	117
Contributor Biographies	143



Leadership without Location: Commanding the Contemporary Operating Environment Beyond the JOC

Battalion Sergeant Major Shane Mc Eneaney

Introduction

The urgency for military leadership to evolve and adapt in today's operating environment arose because traditional centralised command structures face growing vulnerabilities when using fixed Command Posts (CPs) centralised around a Joint Operating Centre (JOC). The electromagnetic spectrum has become “an increasingly congested and contested domain”¹ because adversaries actively work to find, disrupt, or deny access to essential communication and information systems. This makes static command nodes vulnerable to detection, targeting and disruption, undermining the security and effectiveness of traditional Command and Control (C2) arrangements in Multi Domain Operations (MDO). The growing use of advanced electronic warfare capabilities and cyber operations has increased these vulnerabilities. As the “proliferation of disruptive and often dual-use technologies expands the range of options to achieve strategic effect,”² this reality demands a comprehensive review of how armed forces organise, communicate, and make decisions under persistent threat conditions. The move away from fixed JOCs represents both a reaction to technological threats and a transformation of the characteristics of modern warfare. In fact, “the information age has brought new operational requirements which make agility, interoperability and adaptability fundamental attributes for success in full spectrum operations.”³ The traditional hierarchical and centralised command models, which worked well in previous conflicts, no longer meet the requirements of the present day, as Priebe et al state: “21st century operations demand distributed networked resilient command structures, which can maintain effectiveness and operational control, even when individual nodes experience degradation, become isolated or are destroyed.”⁴ The ongoing transformation is further accelerated by Artificial intelligence (AI) working alongside cloud-based operating platforms and wireless sensor networks. But what is AI, and what does it mean for the future of military C2?

Although there is no universally agreed upon definition, Layton's provides a useful description of AI: “a variety of information processing techniques and technologies used to perform a goal-oriented task and the means to reason in pursuit of that task.”⁵ In essence, this means the application of real-time data processing and analytics and the Defence Forces (DF) must adapt to these changes or be left behind by partner nations within the EU and NATO who are implementing Professional Military Education (PME) strategies to train their personnel for the future operating environment. The requirement for decentralised command becomes more evident because of the evolving nature of the battlespace. Modern conflict is characterised by ambiguity and a blurring of traditional boundaries between combatants and non-combatants, as well as between physical and virtual domains. To adapt to this multi-domain operating environment there needs to be a *“departure from the traditional rigid, top-down command structures, embracing a more fluid and*

1 Stéphane Ricciardi and Cédric Souque, “Modern Electromagnetic Spectrum Battlefield: From EMS Global Supremacy to Local Superiority,” PRISM 9, no. 3 (2021): 122-139, 124. <https://www.jstor.org/stable/48640750>.

2 Ministry of Defence, *Integrated Operating Concept* (London: Ministry of Defence, 2021), 16. <https://www.gov.uk/government/publications/the-integrated-operating-concept-2025>

3 David S. Alberts and Richard E. Hayes, *Power to the edge: command... control... in the information age* (Washington DC: Command and Control Research Program, 2003), 8.

4 Miranda Priebe, Meagan L. Smith, Alan J. Vick and Jacob L. Heim, *Distributed Operations in a Contested Environment: Implications for USAF Force Presentation* (Santa Monica, Rand, 2019), 50. https://www.rand.org/pubs/research_reports/RR2959.html

5 Peter Layton, *Fighting Artificial Intelligence Battles Operational Concepts for Future AI-Enabled Wars* (Canberra: The Centre for Defence Research Australian Defence College, 2021), 3. <https://research-repository.griffith.edu.au/bitstreams/b03d79a4-9f5b-43d1-9d8b-52894197b705/download>

dynamic approach to warfare planning and execution."⁶ This will require a shift in mindset from military leadership, moving away from static, process-driven approaches towards more dynamic, information-led, and pre-emptive behaviours. This requires more than just technological innovation; it also necessitates parallel changes to organisational culture, leadership philosophy, and operational doctrine to achieve effective command and control. The future of military leadership and command will be shaped by the integration of advanced technologies and the development of a new operating culture that supports continuous learning and innovation.

Role and Vulnerability of the Joint Operating Centre (JOC)

Functions and Strengths of the Traditional JOC

The JOC operates as the central C2 hub for managing 'current operations', which are typically ongoing activities out to the next 72 hours. The main purpose of the JOC is to offer a secure fixed location where commanders, along with their staff, can coordinate and execute joint campaigns. The JOC allows different service branches and allied forces to work together by synchronising operations across multiple domains, including land, air, maritime, cyber and space. This centralised system enables effective resource management and real-time situational awareness, which supports operational tempo and unity of effort in complex campaigns. Historically, operational synchronisation and decision-making have benefited from centralised, integrated C2 systems, which maximise operational effectiveness and safeguard friendly networks through physical means. However, the risk is now increasingly apparent, as the character of warfare evolves and the vulnerabilities associated with fixed, centralised C2 nodes become more pronounced, necessitating a re-examination of the JOC's configuration in future operations.⁷

Vulnerabilities of Fixed JOCs in the Modern Operating Environment

This section will show that fixed JOCs have become increasingly vulnerable across the Electromagnetic Spectrum (EMS) and digital environment, making them a liability in a contested battlespace. The EMS is now a highly contested and congested space, driven by the growing density and complexity of emissions stemming from the proliferation of digitally enabled weapon and communications systems. As Major General Landrum of the U.S. Air Force observes "the spectrum has become increasingly complex. More players are accessing and leveraging sections of bandwidth, making it congested."⁸ The JOC's EM signature exposes it to a multitude of detection and disruption risks, amplified by their reliance on fixed infrastructure. This exposes them to adversarial Signal Intelligence (SIGINT), which can be used to intercept, geolocate, and target friendly forces.

The integration of artificial intelligence into analytical processes and automation

6 Akshat Upadhyay, "Do-It-Yourself (DIY) Warfare: A New Warfighting Paradigm," *Strategic Analysis* 48, no.1 (2024): 27. <https://doi.org/10.1080/09700161.2024.2331344>

7 Siegfried Ullrich and Sean Moriarty, *Lessons Learned from the Ukrainian Territorial Defense Forces: Command Post Survivability* (Fort Leavenworth: Centre for Army Lessons Learned, 2024), 1. https://www.army.mil/article/273510/lessons_learned_from_the_ukrainian_territorial_defense_forces_command_post_survivability

8 C. Todd Lopez, "As in Other Domains, U.S. Use of Electromagnetic Spectrum Is Contested," U.S. Department of War, 20 May 2020, <https://www.defense.gov/Explore/News/Article/Article/2193532/as-in-other-domains-us-use-of-electromagnetic-spectrum-is-contested>

introduces a dual dynamic; while it offers significant opportunities for enhanced efficiency and decision-making, it simultaneously amplifies the complexity of the security landscape by generating new vulnerabilities and risk vectors. AI, used correctly, supports the transformation of the JOC by enhancing the speed and accuracy of analysis, threat detection, and response. Yet ‘new’ technological solutions must be integrated with strong, system-wide operational security practices, disciplined use of the electromagnetic spectrum, reinforced by continuous review to ensure survivability in contested environments. As Hofstetter and Wojciechowski notes, “In the EW arena; this will take an investment in training, equipment, and a fundamental change in the way the military conducts ground operations.”⁹

Analysis of the conflict in Ukraine further demonstrates the dangers of immobile CPs. In 2022, Ukrainian forces repeatedly struck Russian CPs around the Chornobaivka airfield in Kherson, targeting units across multiple echelons over an eight-month period. These strikes severely degraded Russian command effectiveness and contributed significantly to the collapse of their operational efforts west of the Dnieper River. This negative example highlights the vulnerability of the CP in its traditional configuration, as Engstrom explains: “Western command posts have significant challenges with survivability. Contemporary CPs, with their radio frequency emitting antennas, dozens of generators and vehicles, and extensive support requirements – are easily targetable.”¹⁰ MDO has led to the use of sophisticated cyber capabilities to identify, disrupt or destroy fixed C2 infrastructure. However, while more mobile units in the fighting echelons can rely on agility and adaptability to reposition more rapidly than the adversary, the expansive and static footprint of rear-echelon JOC structures renders them increasingly misaligned with the requirements of such tactics. The Chinese People’s Liberation Army (PLA) explicitly codified this principle in its doctrine and has identified the destruction of adversaries C2 as an essential path to victory. They call it “System Destruction Warfare”, which, they say, “seeks to paralyze and even destroy the critical functions of an enemy’s operational system.”¹¹ According to this theory, the enemy loses the will and ability to resist once its operational system cannot effectively function. The protection of C2 nodes represents an operational necessity because it ensures both freedom of action and operational effectiveness.

At present, C2 architecture is centred around a fixed CP and JOC, which houses all the commander’s staff, including planners, battlespace managers, intelligence analysts, logistics experts and multi-domain liaison officers. This represents a critical vulnerability as it constitutes a single point of failure. The aggregation of personnel, communications infrastructure, and command assets within a single identifiable location creates a critical vulnerability that adversaries can exploit—not only in combat operations but also in the peace support missions to which the DF are routinely deployed. This risk is amplified due to the interconnected nature of military networks, where a breach or disruption can cascade to cause operational paralysis. The future evolution of modern JOCs, as outlined

9 Jerney Hofstetter and Adam Wojciechowski, “Electromagnetic spectrum survivability in large-scale combat operations,” *Infantry* 109, no.4. (2020): 23. https://www.benning.army.mil/infantry/magazine/issues/2020/Winter/PDF/7_Hofstetter_EW.pdf

10 Milford Beagle, Jason C. Slider and. Matthew R. Arrol, “The Graveyard of Command Posts: What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations,” *Military Review* 101. (March 2023): 12. <https://www.armyupress.army.mil/journals/military-review/online-exclusive/2023-ole/the-graveyard-of-command-posts/>

11 Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People’s Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, Rand, 2018), x. <https://apps.dtic.mil/sti/pdfs/AD1085328.pdf>

in RAND Europe's *Command and Control in the Future* concept paper,¹² is largely motivated by the imperative to reduce operational vulnerabilities and enhance resilience. Given current operational risks, it is essential to adopt an information-centric, adaptive, and decentralised C2 model—such as the Ukrainian 'Delta System,' a cloud-based platform that operates via Starlink, or other internet portals, to collect, process and display intelligence on adversary forces, and to deliver situational awareness on friendly forces.¹³ This platform enables the full dispersion of battle staff while preserving situational awareness. By eliminating single points of failure inherent in fixed command posts and JOCs, it reduces the risk that a single strike could incapacitate an entire headquarters and supports leadership diffusion across all command levels.

Leadership Competencies for Decentralised Environments

A critical leadership requirement to implement decentralised command structures is the ability to delegate, empower, and leverage the skills of the tech-savvy young people now enlisting in the armed forces. This starts with doctrine and education as noted by Ryan, who states that: "Given the rapid pace of technological change and the evolution of the demographic profile from which military personnel will be drawn, military institutions must change their approach to professional military learning."¹⁴ Striking the right balance between enforcing a unified doctrinal standard and fostering innovation and trust is challenging, as excessive flexibility risks system fragmentation and inefficiency. Alberts identifies that these challenges may involve a transformation *and* capability development: "Learning the work processes associated with information sharing, exploiting collective knowledge, and conducting the efficient, authoritative collaboration will require establishing new mind sets (education and training) as well as new tools."¹⁵ The challenge lies in establishing interoperable standards that are sufficiently robust to ensure cohesion, yet flexible enough to allow organisations to adapt locally while leveraging diverse capabilities. In summary, the digital transformation of command and control creates additional challenges for standardisation and integration. Advanced military technologies, including AI and autonomous systems, create new interoperability challenges because of varying levels of technological advancement and doctrinal acceptance. Analysis of the Ukraine conflict highlights the necessity of quickly integrating lessons learned from operations into PME and doctrine.

Military organisations typically adopt one of two dominant leadership paradigms: a traditional hierarchical command structure or a mission command-oriented approach. In hierarchical organisations, decision-making authority rests with the superior command element; for example, "Russian command structures follow a hierarchical model which requires strict adherence to centralised directives."¹⁶ In a Mission Command environment,

12 Ellis Conlan, Rebecca Lucas, Martin Robson, James Black, Ben Fawkes, Edward Keedwell, and Alan Brown, *Command and Control in the Future: Concept Paper 3: Conceptualising C2 as a Capability* (Santa Monica: Rand, 2024), 20. <https://policycommons.net/artifacts/14419790/command-and-control-in-the-future/15317686/>

13 Oscar Rosengren, "Network-centric Warfare in Ukraine: The Delta System," Grey Dynamics, 30 August 2024, <https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/>

14 Mick Ryan, *War Transformed: The Future of Twenty First Century Great Power Competition and Conflict* (Annapolis: Naval Institute Press, 2022), 282.

15 Alberts and Hayes, *Power to the Edge*, 90.

16 Victoriano Vicente and Botella Berenguer, "Command and Control Insights from Ukraine," *Finabel - The European Land Force Commanders Organisation*, 23 October 2024, Accessed 19 July 2025, 7. <https://finabel.org/command-and-control-insigh/ts-from-ukraine/>

a “subordinate can and will be free to decide how to execute their mission and task within the framework of the higher commander’s intent.”¹⁷ In summary, aligning diverse leadership models with mission command principles is imperative, as modern distributed command infrastructures require a culture of decentralized decision-making supported by controlled autonomy at all levels of command.

The successful implementation of decentralised C2 in modern military operations depends on mission command principles together with clear articulation of the commander’s intent as Gady and Stronell state:

The mission command philosophy enables centralised planning while executing operations through decentralised methods, which has become essential in the contemporary battlespaces where electromagnetic and cyber domain disruptions threaten traditional command posts and JOCs.¹⁸

This approach gives subordinate leaders the power to decide within the established boundaries of the higher commander’s intent, which results in better adaptability and responsiveness in dynamic operational environments. Mission Command functions through commanders who clearly state their intent so subordinates can have a shared understanding of operational goals and of the commander’s risk appetite. Decentralised decision-making becomes possible through clear communication because commanders at the tactical level receive autonomy to select the best methods for achieving objectives in rapidly changing situations. The Ukrainian Armed Forces have shown how effective this principle is, “where measures were taken to integrate the mission command approach into the military education and training across the services.”¹⁹ This is analysed by Hackett and Nagel, who state, “While Russian centralised command and control was effective in defensive positions, it proved catastrophic during offensive operations. Ukrainian forces, meanwhile, adopted Western-style mission control, this has proven pivotal to Ukraine’s response to Russia’s numerically superior force.”²⁰ By giving more authority to subordinate commanders, they have been able to respond quickly and effectively to battlefield changes.

AI as a Force Multiplier in C2

This section will argue that AI can enhance C2 through the integration of real-time data processing and predictive analytics to improve Situational Awareness (SA), while allowing for dispersed operations and reshaping PME. Real-time data processing and predictive analysis enable commanders to act at an operational tempo that would be unachievable by human analysts alone. As Hackett and Nagel observe, “the Russia-Ukraine War affords vital insights into how future conflicts will be influenced by the abundance of digital information and the maturation of AI.”²¹ Furthermore, AI can be oriented to “evaluate

¹⁷ NATO, *NATO Standard AJP-01 Allied Joint Doctrine* Edition F. (Brussels: NATO Standardisation Office, 2022), 74.

¹⁸ Franz-Stefan Gady and Alexander Stronell, “Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030,” in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. (Brussels: NATO CCDCOE Publications, 2023), 160, <https://kclpure.kcl.ac.uk/portal/en/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis>

¹⁹ “War in Ukraine: Lessons Identified and Learned,” European Values Center, (February 2023), PDF, accessed 25 Sep 25, 11. https://european-values.cz/wp-content/uploads/2023/02/202302-War_in_Ukraine_Lessons_Learned-European_Values_Center.pdf

²⁰ Michael T. Hackett and John A. Nagl, “A Long, Hard Year: Russia-Ukraine War Lessons Learned 2023,” *Parameters* 54, No.3 (2024): 43. <https://doi.org/10.55540/0031-1723.3302>

²¹ Hackett and Nagl, “A Long, Hard Year,” 47.

adversary actions and predict multiple Multi-Domain Operations threat outcomes.”²² The transformation goes beyond technological progress because it intrinsically alters how operational advantage is achieved through information utilisation. AI functions as a force multiplier, extracting useful intelligence that directly affects operational outcomes. This underscores the importance of the technical innovation and organisational adoption, highlighting the planning required for its further integration into command and leadership doctrine and processes. As Mick Ryan suggests, “It is likely to drive greater automation, in turn resulting in changes in training and education to support a more integrated human-machine military institution.”²³ This underscores the need to rethink how PME evolves alongside technological change. As others caution, however, “although AI tools could greatly enhance PME, effective implementation requires understanding of both their capabilities and limitations.”²⁴ In practice, this means re-evaluating how AI is integrated into the military decision-making process without allowing dependence on it to erode human judgement. Indeed, “by leveraging AI-driven simulations, personalised learning, and stress-resilience modelling, PME can enhance realism, adaptability, and decision-making agility.”²⁵ Together, these perspectives highlight the potential of AI as a genuine force multiplier—one that, if harnessed correctly, can strengthen rather than weaken the human element of military effectiveness.

These capabilities also underpin shared situational awareness across dispersed units, an essential requirement for successful C2 in digitally contested battlespaces. NATO’s project Maven exemplifies military efforts to create a “unified interface for battlefield analysis.”²⁶ AI-enabled systems such as Maven, that focus on Intelligence Surveillance and Reconnaissance (ISR), enable quick identification and distribution of essential information about enemy assets and operational environment changes. The capability serves as a critical requirement for units operating at distant locations and experiencing reduced connectivity to maintain a unified operational understanding. As Husain points out, “The combined effect of millions of sensors deployed in space, in the air, on land, on the surface of the sea and under it, all being routed to a scalable AI perception system will be transformative”²⁷ Furthermore, as Davis states, “the rapid expansion of AI’s military applications throughout the world merits a high level of focused attention to ensure maximum advantage.”²⁸ The U.S. Army estimates that “an AI-enabled force has some 10 times more combat power than a non-AI powered force,”²⁹ which illustrates the potential impact of emerging technology on C2 which explains the race to develop systems.

22 NATO, “Multi-Domain Operations and Digital Transformation: Enabling Converging Effects in the Modern Battlespace,” 2 May 2025, Accessed 10 July 2025. <https://www.act.nato.int/article/mdo-dt-enabling-converging-effects/>

23 Ryan. *War Transformed*, 94.

24 Adam T. Briggs, “Enhancing Professional Military Education with AI,” *Journal of Military Learning* (23 April 2025):23, <https://www.armyupress.army.mil/Portals/7/journal-of-military-learning/Archives/April-2025/Enhancing-pme-with-ai/Enhancing-pme-with-ai-UA.pdf>

25 Eric A. Wismar, “Future-Proofing PME: How AI is Redefining Adaptive Wargaming and Strategic Readiness,” *Wild Blue Yonder Online Journal* (20 June 2025), accessed 25 July 2025. <https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/4221801/future-proofing-pme-how-ai-is-redefining-adaptive-wargaming-and-strategic-readiness/>

26 Rizwan Choudhury, “Project Maven: The Epicenter of US’ AI Military Efforts,” *Interesting Engineering* (2 March 2024), accessed 17 July 2025. <https://interestingengineering.com/military/project-maven-the-epicenter-of-us-ai-military-efforts>

27 Amir Husain, “AI is Shaping the Future of War, Institute for National Strategic Security,” *PRISM* 9, no.3 (2023): 53. <https://www.jstor.org/stable/10.2307/48640745>

28 Zachary Davis, “Artificial Intelligence on the Battlefield,” *PRISM* 8, no.2 (2019): 128. <https://www.jstor.org/stable/10.2307/26803234>

29 Peter Layton, “Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled War,” *Joint Studies Paper Series* no.4. (Canberra: Australian Defence Department, 2021). 2. <https://www.defence.gov.au/defence-activities/research-innovation/research-publications/fighting-artificial-intelligence-battles-operational-concepts-future-ai-enabled-war>

Conclusion

This article has argued that the evolution of military C2 systems is essential for navigating the complexities of the contemporary operating environment, which is dominated by rapid technological progress and diverse adversary tactics. Centralised CPs are increasingly vulnerable to cyber, electronic, and kinetic effects and must give way to the adoption of distributed, resilient, and adaptive command frameworks. As David Kirichenko's analysis suggests, "The Russo-Ukrainian War has vividly demonstrated the power of decentralised warfare, establishing a model that will likely shape future conflicts. This new approach, blending traditional military tactics with decentralised networks, has proven highly resilient and adaptable."³⁰ Decentralisation enabled by Mission Command allows multiple decision nodes to function autonomously, improving operational flexibility and responsiveness in contested and dynamic battlespaces.

The structural changes suggested require more than technological advancement. It depends on developing trust-based leadership cultures that empower commanders at every level to make decisions without excessive supervision. Leaders must be confident in delegating authority, even when communications are disrupted. AI integration will strengthen this through the processing of vast data sets at speeds beyond human capacity, enhancing situational awareness and supporting autonomous tactical decision-making. This reduces cognitive strain on operators and improves overall command effectiveness. As one study notes, "AI integration into C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) process results in better indications and warning, information and knowledge management tools, resulting in more reliable intelligence analyses."³¹ At the same time, the future of effective C2 will rest on human-AI collaboration. Frank Hoffman describes this as "System 3 thinking," where "biological-machine intelligence will increasingly be core to the development of the intellectual edge."³² The principle is increasingly evident in the lessons from the Russo-Ukraine war. Both the United States and China have "identified leadership, multidomain integration, signature management, crewed and uncrewed systems and information operations"³³ as decisive factors shaping future conflict.

For the DF, these developments present both challenges and opportunities. They have a unique opportunity to implement the lessons identified from the Ukraine conflict to address capability gaps, such as making greater use of surface, sub-surface and aerial AI-platforms with AI-enhanced battlefield management platforms to optimise and direct targeted operations offers a means to offset the current personnel shortages, maximising operational effectiveness. The High-Level Action Plan for the Report of the Commission on the DF identified five core areas and associated strategic objectives. In relation to the reform of C2, a "New C2 and Joint Structure is to be established."³⁴ This supports the implementation of essential processes and the integration of initiatives that promote

³⁰ David Kirichenko, "Ukraine's decentralized warfare: the battle of the common person," *Asia Times*, 1 November 2024, Accessed 25 June 2025, 8. <https://asiatimes.com/2024/11/ukraines-decentralized-warfare-the-battle-of-the-common-person/>

³¹ István Szabadföldi, "Artificial intelligence in military application – Opportunities and challenges," *Land Forces Academy Review* 21, No.2 (2021): 162. <https://sciendo.com/pdf/10.2478/raft-2021-0022>

³² Ryan, *War Transformed*, 252.

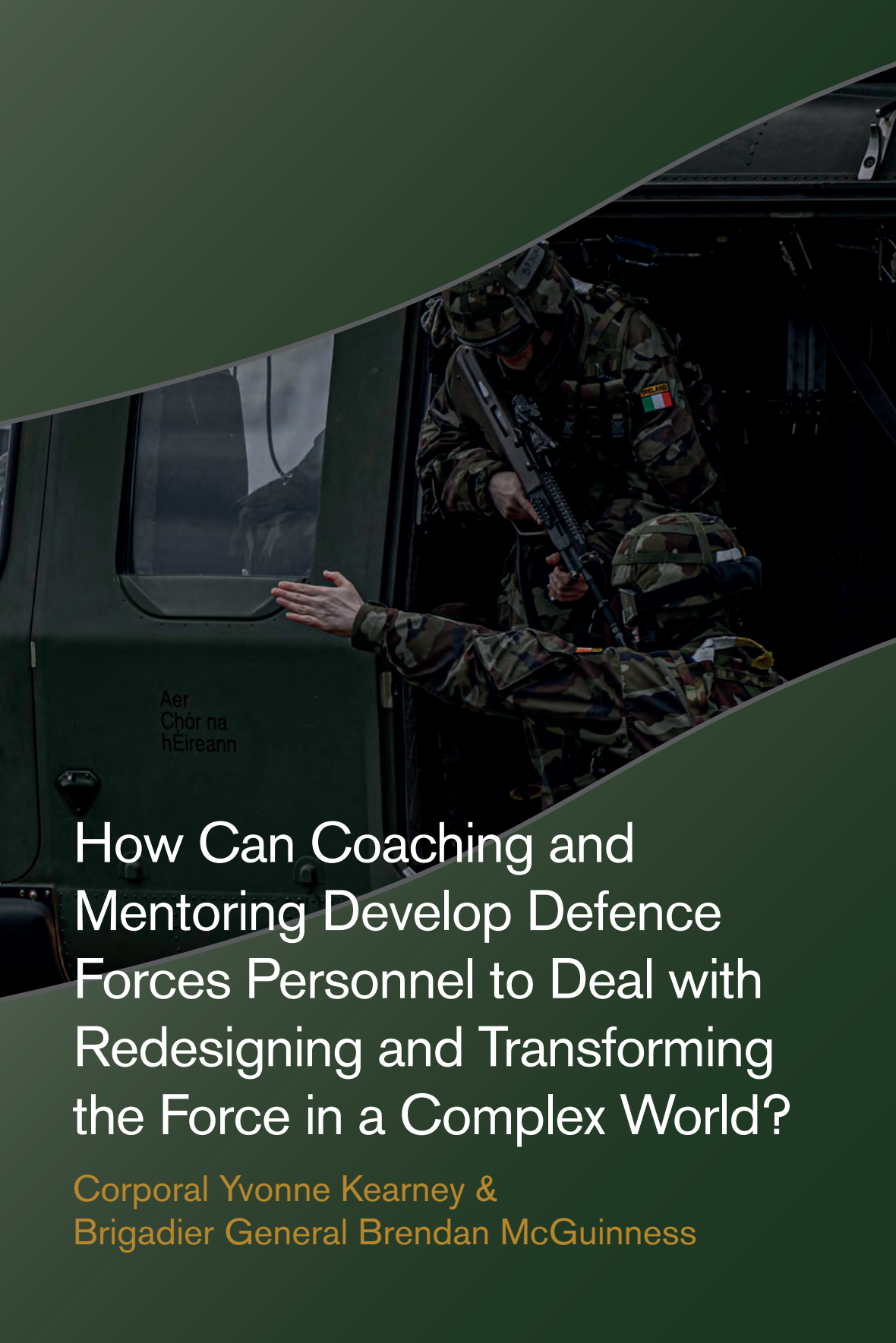
³³ Mick Ryan, *The War for Ukraine: Strategy and Adaptation Under Fire* (Annapolis: Naval Institute Press, 2024), 225.

³⁴ Department of Defence and Defence Forces, *High level Action Plan for the Report of the Commission on the Defence Forces* (Newbridge: Department of Defence, 2022), 9.

modern leadership approaches—particularly those involving technological advancements in training and education. These efforts aim to build confidence in operating within an emerging, dispersed, AI-enhanced command model.

In summary, AI-enhanced battlespace management and human-AI teaming represent not just technological upgrades but institutional and cultural transformations. The DF must embrace these changes to secure a strategic advantage in an increasing complex operating environment, as Beagle *et al.* state: “To optimize our command posts we must reduce our reliance on the physical dimension (the material), increase our utilisation of the information dimension (the data), and maximize our relationship with the human dimension (our leaders).”³⁵

³⁵ Beagle, Slider and Arrol, “The Graveyard of Command Posts,” 17.



How Can Coaching and Mentoring Develop Defence Forces Personnel to Deal with Redesigning and Transforming the Force in a Complex World?

Corporal Yvonne Kearney &
Brigadier General Brendan McGuinness

Introduction

Militaries are designed to function and survive in the extreme exigencies of war. They use robust and clear chains of command and lines of communication to support clearly defined hierarchies of units and ranks. This hierarchical system is designed to make decisions, make best use of resources, generate military effects, and survive and prevail against adversaries in wartime. Langley Sharpe, in *The Habit of Excellence*, perhaps best captures the unique nature of military life:

The institution and those who serve in it are asked to take on responsibilities involving combat, mortal danger and the use of lethal force. Soldiers are required to accept the contract of unlimited liability, accepting the risk to their own life inherent in carrying out their duties.¹

Current defence and security challenges include hybrid warfare, rapidly changing technology and complexity in a post-truth world. In this environment, more agility and flexibility are required while implementing a redesign and transformation of the Defence Forces. The Irish Government's *Defence Policy Review, 2024*, outlines the overarching Strategic level of Ambition as;

To defend Irish sovereignty, protect Irish Citizens and secure Irish interests in support of Irish society, the Irish economy, our collective wellbeing and our territorial integrity. To do so, Ireland requires an agile, modern and fit-for-purpose Defence Forces operating under and in accordance with Defence policy.²

In addressing this complex security and defence environment, this article will focus on presenting the current challenges from internal and external perspectives, describe the Irish Defence Forces (DF) coaching and mentoring programmes, whilst articulating the need for constant communication and practising Mission Command. The potential to develop leaders and decision makers in the organisation through the disciplines of coaching and mentoring, including current internal qualitative data, is followed by a conclusion.

The Challenge

The current national and international context in which the DF and its personnel are serving is complex. This year's DF Review's theme identifies challenges facing defence organisations and personnel; these include hybrid warfare, rapidly emerging technologies, availability of vast data sets, and the concept of a "post truth"³ world. Possible mitigations for DF personnel from the disciplines of coaching and mentoring will be explored.

The current global geostrategic situation includes wars in Europe, the Middle East, and Africa. The UK, NATO, and many EU nations are transforming their military force

¹ Lieutenant Colonel Langley Sharpe, *The Habit of Excellence* (London: Penguin Random House, 2022), 31.

² Government of Ireland, *Defence Policy Review*, (Dublin: Government of Ireland, 2024), 44.

³ Jayson Harsin, "Post-truth and Critical Communication Studies," in *Oxford Research Encyclopedia of Communication* (Oxford University Press, 2018), 5.

readiness with commensurate policy, plans, spending and resourcing of personnel, materiel, and infrastructure. The approach of the United States' administration to world affairs is a constant factor for consideration at the time of writing. Social media offers boundless, accessible information, which in many cases is at best unfiltered, often contains misinformation, and frequently appears as disinformation. Much of this information is designed to "flood the zone,"⁴ influence, and confuse. This methodology can serve the interests of one party and damage the interests of another. Observable in elections, the commercial markets, and in daily discourse, the term 'post-truth' is being applied to this set of circumstances.⁵ To add to the complexity, new defence and security technologies and equipment abound,⁶ and the pace of development and availability is extraordinary relative to recent years. Key themes such as the changing character of war, technological innovations, and bureaucratic challenges are prevalent and are factors in a military leader's decision-making process. The volume of data available adds to the complexity of making timely and well-informed decisions. Conversely, the evolution of AI and technology available to decision makers, if used appropriately and ethically, can assist to counteract the 'flood the zone' methodology. In recent years the term 'VUCA' (volatile, uncertain, complex and ambiguous), has been joined and perhaps overtaken by BANI (brittle, anxious, non-linear and incomprehensible).⁷ These terms seek to encapsulate the state of the wider world, where we as members of the DF find ourselves.⁸ Whatever our role, rank and experience, we are impacted and affected by these phenomena. The military and business literature on leadership⁹ differ in focus on history and traditions, and align on areas such as leadership traits and the potential of effective teams in this complex world. In this pressurised space of leadership and followership, the potential positive impact of coaching and mentoring is significant.¹⁰

The Irish Defence Forces

At the time of writing, the strength of the DF is significantly below the agreed establishment of 9,600. This has implications for all services and personnel in the DF. The organisation is not without its challenges. Cultural, capability, and capacity issues facing the Irish military have been widely reported over recent years.¹¹ However, a significant effort is underway to

4 Peter Aiken, Steve Bannon's 'Flood the Zone' Strategy Explained Amid Trump Policy Blitz, 6 Feb 2025, <https://www.newsweek.com/steve-bannon-flood-zone-strategy-explained-trump-policy-blitz-2027482>

5 Harsin, "Post-Truth," 7.

6 Raj M. Shah and Christopher Kirchhoff, *Unit X: How the Pentagon and Silicon Valley Are Transforming the Future of War* (New York: Simon and Schuster, 2024).

7 Jamais Cascio, *The Innovation Show with Aidan McCullen*, 20 Aug 2024, https://youtu.be/9WY_3H-edsk?si=xGDXUXT4eT1cUw-, 10 Sep 2025.

8 Roman Krznaric, *The Good Ancestor, How To Think Long Term In a Short-Term World*, (London: Penguin Random House, 2021), 43.

9 Sharpe, *The Habit of Excellence*, 241; General Stanley McChrystal, *Team of Teams*, (London: Penguin Random House, 2019), 231-232; Bob Sternfels, Daniel Pachod, and David H. Berger, "Scaling the 21st-Century Leadership Factory," *McKinsey Insights* (2025); Jessica Watson, Peter Evans-Greenwood, Andy Peck, and Peter Williams, *Building the Peloton*, *Deloitte Insights*. 1 July 2020. <https://www.deloitte.com/us/en/insights/topics/talent/high-performance-team-building.html>

10 Dr Shona Brown, Rachel Doogue, Alana Jossel, & Sandy Smith, *Illuminating opportunities for growth in a Team Ecosystem*, 2022, <https://www.coaching-at-work.com/talking-teams-the-team-as-ecosystem/>

11 Commission on the Defence Forces, *Report of the Commission on the Defence Forces*, 9 Feb 2022, <https://www.gov.ie/en/commission-on-the-defence-forces/campaigns/commission-on-the-defence-forces/>;

Independent Review Group – Defence (IRG-DF), *Final Report to the Minister for Defence*, 28 March 2023, <https://assets.gov.ie/static/documents/independent-review-group-final-report-to-the-minister-for-defence.pdf>;

redesign the organisation and transform the culture experienced by its personnel.¹² The current cultural temperature has been taken with a ‘value our people’ survey. The derived and emergent data of this cultural audit will enable the DF to focus its efforts, applying available resources and effort to achieve the desired organisational transformation. Survey briefings indicate a strong interest in coaching and mentoring programmes now and in the future.

There is a palpable sense of urgency about aspects of the transformation that is underpinned Government and DF strategic documents, including the *Strategic Framework*, the Independent Review Group’s *Final Report to the Minister for Defence*, and the *Detailed Implementation Plan*. From a neutral and external perspective, this is understandable, yet in the DF this urgency can translate into a ‘need for speed’, and the requirement for personnel to undertake a number of concurrent roles becomes the norm.¹³ The results of this ‘battle rhythm’ or ‘tempo’ in daily work life can adversely affect balance, and could be mitigated by the implementation of the working time directive (WTD). Paradoxically, the implementation of the approved working time management legislation may be perceived as another task to be achieved. Notwithstanding the existing paucity of time inherent in the current structure, and whilst time is cited in DF data as a predominant barrier to engagement with coaching, the benefits and return on investment (ROI) of time in a coaching engagement are multiple, and often only identifiable either during or after participation.

As personnel endeavour to balance their own working commitments and seek to achieve DF outputs in addition to the transformation agenda at a particular pace, there is a growing sense of challenge in balancing the ambitions and expectations of both individuals and other stakeholders, internal and external to the DF. This set of circumstances brings us to the confluence of the complicated and complex domains where the ‘known unknowns’ and ‘unknown unknowns’¹⁴ have to be accepted. This confluence of international, national and DF external and internal issues bring the BANI impact to many in the DF. How can we bring ourselves to a place of increased self-efficacy, stabilising ourselves and others to manage all that is around and required of us?

For data-supported reasons, the DF has chosen to develop Leaders, Commanders, and decision makers facing these challenges within DF Coaching & Mentoring programmes. One survey of 100 executives reported that the average ROI of executive coaching was six to seven times the cost of coaching.¹⁵ Furthermore, in another survey to derive the benefits of executive coaching, 75% of participants reported that the value of executive and leadership coaching is “considerably greater” or “far greater” than the time and money invested.¹⁶ As there is a significant demand on and ask of leaders during this transformation, coaching

12 Department of Defence, *The Detailed Implementation Plan for the Report of the Commission on the Defence Forces*, November 2023, <https://assets.gov.ie/static/documents/detailed-implementation-plan-for-the-report-of-the-commission-on-the-defence-forces-02.pdf>; Department of Defence, *Strategic Framework: Transformation of the Defence Forces*, September 2023, <https://assets.gov.ie/static/documents/strategic-framework-c29f9bd2-fe4b-495c-9e7e-c6572126046a.pdf>

13 Roman Krznaric, *The Good Ancestor*, (London; Penguin Random House, 2021), 39

14 Joseph Luft and Harry Ingham, “The Johari Window,” *Human Relations Training News* 5, no. 1 (1961): 6-7.

15 Meredith Pratt, “Coaching Statistics: The ROI of Coaching in 2024,” *International Coaching Federation*, 3 September 2024, <https://coaching-federation.org/blog/coaching-statistics-the-roi-of-coaching-in-2024/>

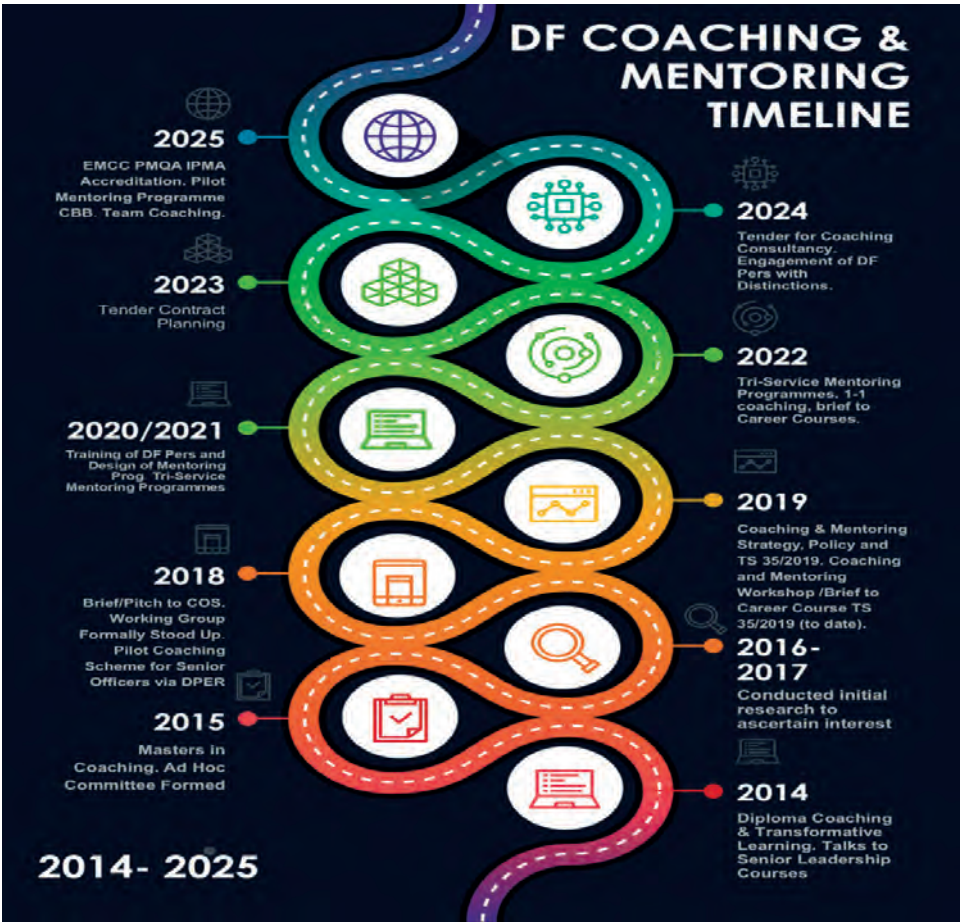
International Coaching Federation, *2025 ICF Global Coaching Study*, 2025, <https://coachingfederation.org/resources/research/global-coaching-study/>

16 Joy McGovern, Michael Lindemann, Monica Vergard, Stacey Murphy, Linda Barker, and Rodney Warrenfeltz, “Maximizing the Impact of Executive Coaching,” *The Manchester Review* 6, no. 1 (2001): 7.

gives back to a leader, offering space and ‘time to think’¹⁷ with a trusted, highly qualified and competent professional.

Coaching and Mentoring Programmes in the Defence Forces

The Defence Forces coaching and mentoring committee has been in place since 2016 and first incepted in 2014. The graphic below¹⁸ outlines the meandering journey taken in the growth and development of these services from one and two people engaged to a small yet dedicated ad hoc committee growing and developing this project in addition to their appointment.



The DF currently has a range of coaching and mentoring programmes underway across the services. The primary reasons the DF engages with and provides coaching and mentoring

¹⁷ Nancy Kline, *Time to Think, An Imperative of Behaviour not Time*, 2005, 3-5, <https://www.timetothink.com/wp-content/uploads/2019/10/te-imperative-of-beha.pdf>
¹⁸ Corporal Yvonne Kearney, Defence Forces Coaching and Mentoring timeline (2025).

are that they are forward-looking, they support personal growth and development, and they allow personnel to access support, appropriate challenge, and systemic wisdom in a transparent and psychologically safe environment. The coaching services are provided by an external professional company called Distinctions Coaching. The services include individual coaching for particular cohorts of personnel across ranks and a team coaching pilot programme. There is both organic mentoring happening across the DF in various workplaces, and this is part of the work traditions of particular units, and in addition, the DF have trained several mentor trainers and mentors to be available in all services, facilitating formal mentoring relationships when requested.

In the *Defence Forces Leadership Doctrine* John Whitmore's definition of coaching is offered as "unlocking people's potential to maximise their own performance. It is helping them to learn rather than teaching them."¹⁹ The same document adopts David Clutterbuck's definition of a mentor as "a more experienced individual willing to share knowledge with someone less experienced in a relationship of mutual trust."²⁰

The vision for coaching and mentoring in the DF is for the programmes to grow and become available to a wider number of personnel. This includes the formal accreditation of the DF coaching and mentoring programmes with the European Mentoring and Coaching Council (EMCC). This work is ongoing and being led by the new Coaching and Mentoring Programme Manager, supported by the DF coaching and mentoring committee. Another aspect of the vision is to have coaching available to a wider and more focused group of personnel across all services and ranks. In addition, more proactive communication will ensure a common understanding of the services, their benefits, and differences.

Both disciplines offer personnel the opportunity to speak in confidence to a trusted person of their choice with a view to developing and growing themselves or dealing with a current question or challenge in their service or work environment. Coaching and mentoring could be viewed as on a scale²¹ as depicted in the graphic below. The coaching is conducted with a professional and qualified coach over a defined time period, while the mentoring is normally less formal and can be spread across an agreed period or series of conversations. In both cases, the person seeking the support should be leading the engagement to get what they need with the coach or mentor in support and available to use their skills and or experience. To date, the anonymous and qualitative feedback from the vast majority of coaching delivered is positive and indicates that the DF and its personnel need and want this service. This strongly indicates that coaching works in terms of supporting those engaged in their development goals and in moving forward in their professional and other aspects of life.

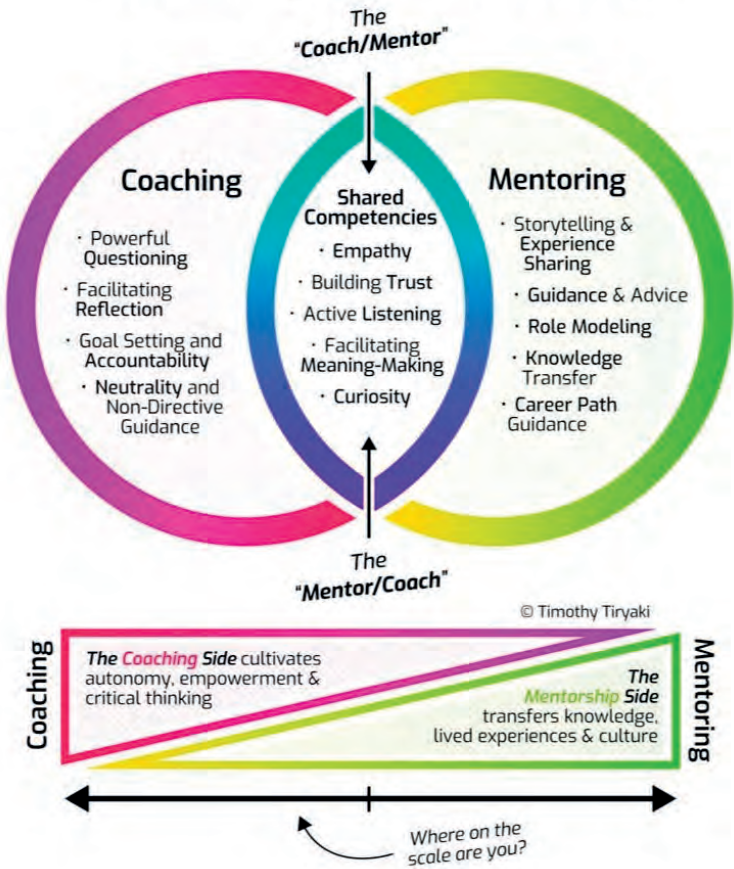
¹⁹ John Whitmore, *Coaching for Performance* (London: Nicholas Brealey, 2009), as quoted in Irish Defence Forces, *Defence Forces Leadership Doctrine DFDM J-2*, Second Edition (Dublin: Defence Forces, 2024), 30.

²⁰ David Clutterbuck, *Everyone Needs a Mentor* (London: CIPD, 2019), as quoted in Irish Defence Forces, *Leadership Doctrine*, 30.

²¹ Reproduced with permission from the Author. Dr. Timothy Timur Tiryaki, *Leading with Strategy: Using Your North Star to Guide Decision-Making* (Canada, Wiley, 2026).

Coaching vs. Mentorship

Understanding the differences and why



It is timely to energeise, overtly advertise, and encourage DF personnel to avail themselves of these services. The current transformation process and initiation of the Detailed Implementation Plan emerging from the Commission on the Defence Forces is the perfect time to institute coaching and mentoring into the new HR architecture of the DF. Currently, there is a need to have leaders and decision makers empowered to use Mission Command, rely on their training and experience, and have the handrails of coaching and mentoring available.

Communication and Mission Command

In recent years, communications has been prioritised across the DF with the rollout of an internal digital platform, 'Workvivo', a range of new meetings, engagements and use of many media platforms. Endeavouring to improve communications is not uncommon across organisations. In militaries, there are other factors that can overlay this, namely the balance of power as represented by rank and appointment and the concept of seniority. If these are out of balance or inconsistent with values or changing cultural priorities, it can cause confusion among personnel and friction in the DF system. Within most Western militaries, the concept of Mission Command is important to empower personnel in executing tasks and operations when appropriate. It is a philosophy of command and leadership that promotes decentralised decision-making by subordinates, as long as it is aligned with their superior commander's intent.²² This is a concept that is taught and espoused in the DF, and when practiced, should empower and provide freedom of action to personnel.

Focused military operations and practices supported by doctrine, training and deployments are imperative in wartime, yet run the risk of being perceived as micromanagement if carried into day-to-day peacetime service. Currently, decision makers and leaders are required to manage and lead in differing circumstances that include constant data flow, changing transformational demands and priorities, and a need to maintain and improve communications. There are many mechanisms available to enable and empower personnel to become more self-aware and increase self-efficacy, while dealing with the challenges outlined, one of which is coaching.

In these situations, forward looking developmentally focused coaching relationships in the Defence Forces One-to-One Executive Coaching programme,²³ have demonstrated the effectiveness of a coaching relationship to enhance specific areas related to current challenges. One participant reported that their experience of coaching: "Provided a refined focus on initiatives I wish to achieve. Created a clear roadmap for the coming months. Assisted in answering and focusing me to be in a better position to answer the 'WHY' to many questions related to DF transformation."²⁴ In the qualitative feedback data, another participant commented that: "The ability to honestly discuss issues and to be challenged and encouraged in equal measure is highly effective. The confidential nature of the service is very reassuring..."²⁵ Furthermore, one participant felt they had gained "A deepened understanding of how a leadership approach impacts a team's performance."²⁶

Crucially, this feedback can assist the senior DF leadership as they seek to identify the current climate and culture in the organisation. This new information supports the long-standing data and feedback from multiple sources, such as surveys, 'townhall' talks to troops by general officers, and feedback from the chain of command.

²² Irish Defence Forces, *Leadership Doctrine*, 35.

²³ DF one-to-one executive coaching programme aggregated, themed and anonymous feedback from coaching consultancy (June, 2025).

²⁴ DF one-to-one executive coaching, feedback.

²⁵ DF one-to-one executive coaching, feedback.

²⁶ DF one-to-one executive coaching, feedback.

Potential of Coaching for Leader Development

Coaching has the potential to develop leaders and decision makers across all levels of the DF. Of course, there are also limitations to what coaching can achieve or deliver within resource, time, and contract parameters. For example, one-to-one coaching can have a reasonably quick and, in many cases, lasting effect on the individual and, by extension, the organisation that those personnel operate in. A coaching formula of ‘performance = potential – interference’²⁷ encapsulates a key goal of coaching at the individual level. Removing internal obstacles creates space for increased learning and performance. If the effect is positive and it brings about changes in self-awareness, thinking, feeling and relational working style of the coachees it can ripple positively across the network of the coachees for the duration of their careers. The limitations associated with one-to-one coaching are that it may only be impactful with the coachee and also may only last for the duration of the coaching relationship. There is no guarantee of how coaching will impact, however if framed as a positive self and organisational development opportunity it can nudge the process in the positive direction. This is supported by the previously mentioned data emergent from DF one-to-one executive coaching programme June 2025.

Coaching at both an individual and team level offers an opportunity to unearth potential unconscious effects of culture and the wider system on DF leaders, enhancing emotional intelligence. As transformation is prevalent and unrelenting, the capacity for self-awareness, self-management, social awareness, and relationship management²⁸ are arguably imperative in the current environment. In an era of AI centric communication, psychologist Martyn Newman proposes that it is our humanity that provides a necessary counterbalance to emergent and fast changing technology, particularly in the context of leadership.²⁹ Coaching offers the opportunity to increase cognitive flexibility, critical thinking, reflection, and the capacity to respond and adapt to technological advances and emergent situations. Within the context of a coaching relationship, leaders are offered space and time to think, to interrogate cognitive biases and mind maps, and investigate habitual responses, emotions, behaviours, strengths, and limitations. An increase in self and other awareness and management, such as empathy³⁰ can assist to develop confidence in leaning into strengths and addressing limitations. Once considered a ‘soft skill’ or a nice but not necessary attribute, emotional intelligence is now deemed a ‘power skill’ where human centric leadership can support teams and encourage innovation.

Coaching is now considered a vital component of leadership development and in the DF it is currently offered at executive leadership level as a unique opportunity to invest time for development. As Goldsmith contends, the higher the leader, the higher the priority for awareness of interpersonal behaviour; ‘what got you here won’t get you there’.³¹ As a forward looking, empowering endeavour, coaching can assist to bridge the

27 W. Timothy Gallwey, *The Inner Game of Work* (London: Random House, 2001), 18.

28 Lucas Filice and W Weese, “Developing Emotional Intelligence.” *Encyclopedia* 4 no. 1 (2024): 583.

29 Martyn Newman, “EQ in the Age of AI: What Smart People Know That Machines Never Will,” Online website video, 11.35-12.43, 28 Aug 2024. <https://www.rochemartin.com/videos/eqintheageofai>

30 Hera Antonopoulou, “The Value of Emotional Intelligence: Self-Awareness, Self-Regulation, Motivation, and Empathy as Key Components,” *Technium Education and Humanities* 8 (2024): 78. https://www.researchgate.net/publication/379764627_The_Value_of_Emotional_Intelligence_Self-Awareness_Self-Regulation_Motivation_and_Empathy_as_Key_Components

31 Marshall Goldsmith and Mark Reiter, *What Got You Here Won’t Get You There: How Successful People Become Even More Successful* (London: Profile Books LTD, 2013), 21.

gap between being near great and great, especially in times of rapid transformation and change. Furthermore, a coaching leadership style can be adopted when situationally appropriate by leaders seeking to empower and develop other leaders.³² Achieved through active listening, asking rather than telling, and encouraging others thinking to develop their own solutions, this is particularly valuable when innovation and creativity are necessary to overcome current challenges, especially in a team context.

Team coaching can support teams aligned to a common purpose and with an inspiring vision. It can provide role clarity, help the team with accountability, to make powerful choices, resolve conflict and take affirmative action. When appropriately framed and delivered, team coaching can have an impactful ripple effect on teams and their work. It also affects a greater range of ranks and personnel relative to the one-to-one coaching. This leads to conversations within the team that can focus on dynamics at work, how trust is established or broken, and what psychological safety looks and feels like. In conjunction with the one-to-one coaching programme and the mentoring programme it offers an opportunity for wider leadership development.

Potential of Mentoring for Leader Development

Mentoring is a proven, powerful enabler for organisations and personnel by supporting self-directed learning, growth and improving personal performance. Mentoring has been organically available in the DF for many years with particular units, corps and services who use this methodology to pass on skills and capability.

The mentor role is defined by “intention, relationship and circumstances.”³³ Mentoring continues to benefit personnel, however this is occasionally on a more ad hoc basis where there are some personnel that do not have ready access to mentoring relationships. The DF coaching and mentoring committee have taken steps to improve this situation, including *inter alia*: promulgation of a DF Coaching and Mentoring strategy and policy document which includes the management, governance and quality assurance structures that are in place;³⁴ increasing accessibility to formal mentoring via mentor trainers in each service/formation; and engagement with external partners such as the New Zealand Air Force, to explore and learn from their successful implementation of formal mentoring programmes for leader development.

The question posed above is how to develop DF leaders and decision makers during redesign and transformation in this world of complexity. Mentoring, whether ad hoc or formal, based on an open, positive and helping relationship between two people who agree to engage, has the potential to develop DF leaders and facilitate the growth of confidence, purpose, and insight in both the mentee and the mentor.³⁵ Reverse mentoring is a relationship where a junior or younger employee mentors a senior or older employee, reversing the traditional dynamic; ideally, present in all such relationships. This facilitates

³² Irish Defence Forces, *Leadership Doctrine*, 132-135.

³³ Julie Starr, *The Mentoring Manual. Your step-by-step guide to being a better mentor* (London: Pearson, 2014), 66

³⁴ Irish Defence Forces, *Coaching and Mentoring Policy for the Irish Defence Forces (2023-2026)*, 4-5.

³⁵ Irish Defence Forces, *Leadership Doctrine*, 115.

more experienced individuals in gaining fresh perspectives and developing new skills, particularly in areas like technology, social media, and digital practices. Ensuring access to mentoring relationships is a key senior leadership responsibility as the DF seeks to recruit and retain to achieve the desired and mandated redesign and transformation. All leaders can support mentoring by amplifying the potential of mentoring and modelling being a mentee and or a mentor.

Conclusion

Our leaders and decision makers are exposed to constant flows of data and requirements from the internal transformation agenda and external oversight requirements. The imperative to embrace new technology exerts additional demands while delivering organisational outputs. This set of circumstances is exacerbated as the organisation is below its established strength. The DF is navigating this complex and challenging environment with an emphasis on retaining historical strengths and positive traditions, whilst concurrently embracing change. The Coaching and Mentoring Programmes provide an opportunity to enhance transformation, through the development and growth of leaders and decision makers. The qualitative data emergent begins to offer evidence of personal development and growth, and as yet uncharted organisational transformational potential, particularly with team coaching. The DF has embedded coaching and mentoring in Strategic HR and is applying significant resources to enhance operational capability as a counter-balance in a complex world through the vector of its people. In the authors' view coaching and mentoring have a key role in developing our leaders and decision makers to lead and manage the ongoing DF transformation and meet the challenges of the contemporary operating environment.

How Can Coaching and Mentoring Develop Defence Forces Personnel to Deal with Redesigning and Transforming the Force in a Complex World?



Educating the Modern Leader - Embracing Informal Learning in the Irish Defence Forces

Corporal (AR) Fearghal Fitzgibbon

Introduction

The nature of military leadership is currently being reshaped by a rapidly evolving global landscape.¹ The contemporary operating environment is dominated by accelerated technological change, hybrid warfare, and information disorder.² Increased pressure is placed on junior leaders to not only display tactical competence but also digital literacy. Traditional military education systems remain vital, but they are increasingly being supplemented, and in some cases supplanted, by informal and decentralised forms of learning. Podcasts, veteran-led social media, *You Tube* channels, and AI platforms now offer junior NCOs and officers rapid access to military history, doctrine, leadership insights, and tactical analysis that extends beyond the classroom or training ground.

This article argues that the Irish Defence Forces (DF) should not only support, but actively engage with, the informal learning behaviours of junior leaders, because it is already happening. Some level of oversight is required to prevent the inherent risks of unsupervised informal learning. It examines how informal learning is handled in other militaries and civilian organisations to see how it could be integrated into professional military education and continuous professional development.³ It will also consider the risks of unregulated learning and propose strategies that can be used to mitigate this. It argues for a continued hybrid learning model where the standard traditional professional military education works alongside instilling a culture of informal learning and continuous professional development. This hybrid approach has the potential to enhance individual capability across the organisation and develop critical thinking skills. It is also in line with the DF's own approach to promoting blended learning across the organisation.⁴

The Changing Learning Environment

Advancements in technology and pedagogy have changed the learning environment. Globally, in both civilian and military contexts, there is a shift towards student-centred learning that prioritises their needs, autonomy, and preferences.⁵ Educators are expected to differentiate their teaching to meet the needs of individual learners.⁶ They are shifting to being facilitators that assist student-directed learning as opposed to the traditional method of being a knowledge provider.⁷ This shift has not been solely confined to the civilian world. Military education, too, has been affected as institutions seek to modernise their professional development frameworks.⁸ They must adapt to a generational shift as junior military leaders are now drawn from Generation Z and digital natives. Their expectations of leadership, learning,

1 Tang Meng Kit, "Narratives under Fire: Information Warfare Lessons from India–Pakistan and Ukraine–Russia," *Small Wars Journal*, July 31, 2025, <https://smallwarsjournal.com/2025/07/31/information-warfare-lessons/>.

2 Iain Cruickshank and Michael Schwillie, "Beyond Collection: Building Publicly Available Information Systems for Strategic Effect," *Small Wars Journal*, April 29, 2025, <https://smallwarsjournal.com/2025/04/29/beyond-collection-building-publicly-available-information-s/>.

3 Megan J. Hennessy, "How Can We Know IF Professional Military Education Works?" *War on the Rocks*, August 3, 2020, <https://warontherocks.com/2020/08/how-can-we-know-if-professional-military-education-works/>.

4 Defence Forces Ireland, *Defence Forces Professional Military Education Strategy 2021–2025* (Dublin: Defence Forces, 2021): 13, 21, https://www.military.ie/en/members-area/members-area-files/20210302_defence-forces-professional-military-education-strategy.pdf

5 Susan Watts-Taffe, B. P. (Barbara) Laster, Laura Broach, Barbara Marinak, Carol McDonald Connor, and Doris Walker-Dalhousie, "Differentiated Instruction: Making Informed Teacher Decisions," *The Reading Teacher* 66, no. 4 (2012): 305, <http://www.jstor.org/stable/23321311>.

6 Kathryn Young and Kathleen Luttenegger, "Planning 'Lessons for Everybody' in Secondary Classrooms," *American Secondary Education* 43, no. 1 (2014): 27 <http://www.jstor.org/stable/43694200>.

7 Watts-Taffe et al., "Differentiated Instruction," 305.

8 Herbert H. Bell and Charles M. Reigeluth, "Paradigm Change in Military Education and Training," *Educational Technology* 54, no. 3 (2014): 53, <http://www.jstor.org/stable/44430274>.

and professional growth are different from those of previous generations in accordance with shifts in education. They expect a coaching or mentoring style rather than a purely authoritarian one, as is traditionally associated with the military.⁹

The most recent DF Joint Professional Military Education (JPME) recognises that the majority of current inductees are now digital natives from Generation Z who have never known a world without the internet.¹⁰ Traditional approaches to military education must evolve. The JPME Strategy aims to expand the DF's use of technology in learning, "particularly for simulation, virtual reality, augmented reality, and blended learning."¹¹ Military education presents several unique challenges that civilian education does not have to face.¹² JPME is the DF's system of training and education designed to develop the military capabilities of the organisation, so that the DF can provide for the military defence of the State, contribute to national and international peace and security, and fulfil all other roles assigned by the Government. Professional military education (PME), the world over, is formalised through structured courses. It is an ordered environment with set topics to be covered, from an approved syllabus, with assessments throughout. This is the traditional form of PME in militaries worldwide.¹³ In the Irish context, this is represented by recruit training, the cadet school, NCO development, skills courses, and more. This structure also allows accreditation for career advancement courses by recognised civilian academic institutions. This traditional model of education provides a standardised foundation in military doctrine, discipline, and professionalism.¹⁴ The communal shared experience builds a group bond amongst students, while face-to-face contact ensures instructors can closely monitor their progress.

However, while formal military education remains essential, it cannot respond with the same level of speed or flexibility as decentralised learning platforms that currently dominate the information environment.¹⁵ Many junior leaders in the military now rely increasingly on informal learning from these sources. It is typically self-directed, interest-driven, and opportunistic. It occurs through military podcasts, *YouTube* videos, online discussions, social media interactions, and even AI-based tools. For many younger personnel, this is their primary mode of accessing military history, doctrine, and leadership ideas. The speed and extent of informal platforms mean they can expose learners to perspectives, case studies, and emerging lessons far faster than a more rigid institutional system can adapt.

9 SFCR Hanks, "What Soldiers Want: The Gen Z Perspective," *NCO Journal*, (February 2022), accessed August 2025, <https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2022/February/What-Soldiers-Want/>

10 *Defence Forces Joint Professional Military Education (JPME) Strategy 2025–2028* (Dublin: Public Relations Section, Chief of Staff's Branch, 2025), 42.

11 *Defence Forces JPME Strategy 2025–2028*, 42.

12 Government of Australia, "Evolving an Intellectual Edge: Professional Military Education for the Australian Army" (accessed June 20, 2025), <https://cove.army.gov.au/sites/default/files/10-12/11/Evolving-an-Intellectual-Edge-Professional-Military-Education-for-the-Australian-Army.pdf>.

13 John F. Troxell, "The Moldovan Military Academy: Transforming Officer Education," *Connections* 11, no. 4 (2012): 100, <http://www.jstor.org/stable/26326303>.

14 Robert Gibson, "How to Create Professional Military Education (PME) | The Cove," *The Cove*, June 14, 2022, <https://cove.army.gov.au/article/how-create-professional-military-education>.

15 David S. Maxwell, "Thoughts on Professional Military Education: After 9-11, Iraq, and Afghanistan in the Era of Fiscal Austerity," *Small Wars Journal* (Arizona State University), November 14, 2024, <https://smallwarsjournal.com/2012/01/01/thoughts-professional-military-education-after-9-11-iraq-and-afghanistan-era-fiscal/>.

Informal learning refers to the acquisition of knowledge and skills that occurs outside of formal educational settings such as classrooms.¹⁶ It is usually unstructured, self-directed, and driven by individual interest or needs. Informal learning can occur in various everyday situations, such as through social interactions, personal experiences, online videos, or even social media. It is particularly associated with Generation Z.¹⁷ This can manifest itself in many ways in the military context. Social media and the digital age have allowed the world's population to watch conflicts in real time. Soldiers can now view combat footage from the frontline uploaded the very same day via social media or OSINT platforms.¹⁸ Others may listen to veteran led podcasts or review historical conflicts through video essays or blogs. A reservist could use online platforms such as *Reddit* or *Discord* to engage in discussion relating to fieldcraft or tactics. This online proliferation of military content enables junior leaders to engage with operational concepts before they are formally introduced to them in a classroom setting on a military course.¹⁹

While this offers great potential to the development of junior military leaders, it also presents challenges. Informal learning lacks institutional oversight, which can lead to fragmented understanding of a topic or exposure to misinformation. Without structured reflection or guidance, learners may struggle to separate credible insights from mere entertainment or ideologically biased content. Soldiers and junior leaders may not be aware of the reliability or credibility of the sources they consume, whether this be online discussions or video footage. There is also a risk that they will diverge from established doctrine, tactics, techniques, and procedures (TTPs). While informal learning can be a valuable asset to soldier development, it also poses several risks, as soldiers may not fully understand the context of what they consume.

Nonetheless, this evolution cannot be ignored by military institutions.²⁰ Informal learning has already taken root, and its influence will only grow with the generational shift in the DF. The question is no longer whether to engage with it, but how to shape and guide in a way that will complement and enhance the traditional military education currently in place.

16 Barbara Rogoff, Maureen Callanan, Kris D. Gutiérrez, and Frederick Erickson, "The Organization of Informal Learning," *Review of Research in Education* 40 (2016): 356, <http://www.jstor.org/stable/44686827>.

17 Theresa Conefrey, "Technology in the College Classroom: Crisis and Opportunity," *Educational Technology* 56, no. 4 (2016): 38, <http://www.jstor.org/stable/44430476>.

18 David Acosta, "Are We Informationally Disadvantaged? The Realities of Information War in Ukraine," *Small Wars Journal* (Arizona State University), May 9, 2022, <https://smallwarsjournal.com/2022/05/09/are-we-informationally-disadvantaged-realities-information-war-ukraine/>.

19 Andrea Tullos, "Making Professional Military Education More Agile in the Air Force," *War on the Rocks*, June 19, 2025, <https://warontherocks.com/2025/06/making-professional-military-education-more-agile-in-the-air-force/>.

20 Chris Johnson, "Professional Military Education Is PT for the Brain," *From the Green Notebook*, June 19, 2024, <https://fromthegreennotebook.com/2024/06/19/professional-military-education-is-pt-for-the-brain/#:~:text=The%20Australian%20Army%20defines%20PME,peers%20on%20our%20own%20time.>

Informal Learning in Practice – Military Examples

Informal learning is already in practice within the DF. For example, the DF Podcast, which has run since 2020, provides interviews and discussions with serving personnel, veterans, and subject matter experts.²¹ It allows members of the organisation to access professional insights in an accessible format, often outside working hours. Beyond this, personnel with access to manuals and training materials frequently review them in their own time, motivated by personal interest or preparation for future roles. Instructors in specialist areas—such as tactics, heavy weapons, or communications—routinely stay current with TTPs, international best practice, and lessons from ongoing global conflicts.²² The DF acknowledges that military professionals need a combination of training, education, informal, and experiential learning to perform effectively in the contemporary operating environment.²³ This is exemplified through both doctrine and practice.

Lessons can also be learnt from foreign militaries and their efforts to support informal learning and continuous professional development. Both the Australian and Canadian militaries maintain online platforms to support PME. These are aimed at serving members, and designed to upskill and enhance their individual learning experiences. These examples are particularly relevant, as similar to Ireland, they are primarily English speaking.

The Australian platform, *The Cove*,²⁴ is a particularly well-developed resource. It facilitates access to learning materials and events that relate to the profession of arms. User participation is actively encouraged in order to share personal views, knowledge, and experience. It aims to connect soldiers and promote continuous professional development. *The Cove* is particularly noteworthy as it encourages submissions from all ranks, including those from outside the Australian Defence Force. It offers numerous learning modules that learners can engage with at their own pace.

The Cove is partnered with the Queensland University of Technology (QUT) and currently provides 93 learning modules for serving members. All the modules meet equivalent standards on the Australian Qualifications Framework. A multimedia approach is utilised to cater to different learning styles and ensure an engaging learning experience for students. As recognition of learning, *The Cove* offers digital badges that can be displayed on *LinkedIn* and CVs. Learners can complete a formal assessment to qualify. They also provide a reflective journal application to assist learners in creating a habit of reflective practice. A heavy emphasis is placed on this in order to encourage flexible thinking and evaluation.

The Canadian Army equivalent is *Line of Sight*. It is open to all personnel but predominantly aimed at junior officers and NCOs. Similar to *The Cove*, a heavy emphasis is placed on self-directed learning, sharing of insights, and development of problem-solving skills. Modules are focused “on professional development with the stated goal being the creation and

21 Defence Forces Ireland, “Defence Forces Podcast, Season 1,” accessed August 15, 2025, <https://www.military.ie/en/members-area/social-media-links/df-podcast/season-1/>.

22 Heidi Hardt, “Lessons Learned, Lessons Forgotten? Updating the Way NATO Learns,” *War on the Rocks*, July 10, 2018, <https://warontherocks.com/2018/07/lessons-learned-lessons-forgotten-updating-the-way-nato-learns/>.

23 Defence Forces JPME Strategy 2025–2028, 19.

24 Government of Australia, *The Cove*, accessed May 29, 2025, <https://cove.army.gov.au/>.

sustainment of a sense of professional curiosity and career-long learning.”²⁵ Similar to the Australian military, the Canadian Army believes in informal learning and professional self-development. It also recognises that informal learning in the military context “must be interesting, relevant, incentivised, and rewarding.”²⁶ The DF could look to these platforms as models for developing its own dedicated online learning hub for serving personnel. Since much of the content on platforms like *The Cove* and *Line of Sight* is publicly accessible, the DF can readily examine these initiatives and draw inspiration from their structure, content, and engagement strategies.

Informal learning can be a fantastic asset due to its flexibility and real-world experience. However, there are also risks associated with it, particularly in the military learning environment. The collected theoretical and technical knowledge of a military is its doctrine, and this is learned by its members through specialised training and education. The collected theoretical and technical knowledge of a military organisation—its doctrine—is carefully developed through research, operational experience, and strategic intent. An informal learner in the military context must develop critical thinking skills in order not to rely on inaccurate or misleading information. While a certain amount of autonomy is granted to instructors, they must not be at odds with doctrine or standard operating procedures as a result of learning from sources outside of the Irish military.

Informal learning, by contrast, is often decentralised, unverified, and shaped by personal preference. Learners will naturally gravitate towards topics they enjoy rather than focusing on improving deficiencies in their training. Without proper critical thinking and evaluation skills, individuals may absorb misleading, outdated, or overly simplified information. This is particularly dangerous in a military context where poor decision-making or deviation from doctrine can have significant operational consequences. Instructors and junior leaders may unintentionally introduce practices or ideas from foreign armed forces, online influencers, or popularised “tacticool” content that conflict with DF doctrine or standards.²⁷

Informal Learning in Civilian Professions

The DF can also learn from other public sector bodies, drawing valuable lessons from how external organisations encourage continuous professional development (CPD). Numerous branches of the public sector have institutionalised their own CPD frameworks to stimulate professional development. In Ireland, Medical doctors are legally obliged to maintain their professional competence by enrolling in professional competence schemes; the requirements of which are set by the Irish Medical Council (IMC).²⁸ A wide variety of courses are available to doctors, and they must log a minimum of 50 hours every year. This CPD must also include a practice review, such as an audit. All of the CPD activities

²⁵ National Defence, “Government of Canada,” *Line of Sight – Canada.ca / Gouvernement du Canada*, July 15, 2025, <https://www.canada.ca/en/army/services/line-sight.html>.

²⁶ National Defence, “Government of Canada.”

²⁷ Wiktionary, s.v. “tacticool,” last modified August 12, 2025, <https://en.wiktionary.org/wiki/tacticool>.

²⁸ Royal College of Physicians of Ireland, “Home,” accessed May 18, 2025, <https://www.rcpi.ie/Learn-and-Develop/Lifelong-Learning/Professional-Competence/What-You-Need-to-Know-about-Professional-Competence/Your-Professional-Competence-Requirements>.

must be recorded on an online platform provided by the IMC. Some of these are formal learning activities on accredited courses, whereas others are self-directed, such as a personal professional development plan, work-based learning activities, or personal research.

A different approach is taken by the Department of Education. Teachers are encouraged to complete up to three CPD courses every summer as part of their self-development. Similar to the Medical Council, these courses must be approved by the Department. Completion is not mandatory, but those who do take part can earn up to five extra paid vacation days for the following year. There is no restriction placed on the type of courses; it is up to each individual teacher to choose which type of course they wish to complete. Many teachers use this as an opportunity to improve on areas which they feel are deficient or specialise in new fields. The private sector takes another approach, in particular, the world of IT. Tech workers place a heavy reliance on informal learning through the use of online courses and peer forums such as *GitHub*.²⁹

A potential way of introducing this in a DF context would be to take inspiration from the two public service examples described above. A method of logging CPD hours could be instituted, and those who meet certain minimum requirements can then be rewarded with incentives such as days in lieu. A restrictive mandatory approach would defeat the purpose. Learners should be encouraged to engage with the CPD and given an incentive by some form of reward or recompense for the time committed.

Drawing inspiration from informal learning structures of other organisations, the DF can harness their success and devise a strategy aligned with the nuances of military life. This would enable the DF to devise a bespoke system to suit its needs and to cultivate a culture of lifelong learning that empowers its personnel and strengthens the organisation's overall capability.

Opportunities: Institutional Engagement and Hybrid Learning Models

Both the previous and current DF PME strategies have acknowledged the need for reform, but the JPME Strategy 2025–2028 marks a decisive shift toward embracing new learning paradigms.

Innovations include expanding the role of hybrid, blended, and online learning models. Modularisation and micro credentials are also being explored as an alternative to long continuous attendance.³⁰ This has already been successfully applied in preparatory instructional courses for those involved in inductee training and NCO career advancement courses. Specialised weapons instructor training, where students qualify as instructors on

29 Christopher Scaffidi, "Studying in the 'Bazaar': An Exploratory Study of Crowdsourced Learning in GitHub," *Journal of Systems and Software* 149 (2019): 150, https://www.researchgate.net/publication/332947736_Studying_in_the_'Bazaar'_An_Exploratory_Study_of_Crowdsourced_Learning_in_GitHub

30 Gary Schaub, Henrik Ø. Breitenbach, and Flemming Pradhan-Blach, "Professional Military Education: A National Affair," in *Invading Bologna: Prospects for Nordic Cooperation on Professional Military Education* (Copenhagen: Centre for Military Studies, 2013), 19, <http://www.jstor.org/stable/resrep05277.5>.

several weapons systems, have been modularised into individual courses focused on a single weapon, which are shorter in length. This allows NCOs and officers the opportunity to upskill themselves while reducing their time away from their unit or home.

Blended learning is intended to address some of the issues regarding retention, access to courses, and improving the work-life balance. It will also be of particular benefit to the Reserve Defence Forces (RDF), who generally train during weekends or holidays. This has already been experimented with as several career advancement courses have incorporated distance learning, and other courses, such as specialised instructor training, have been run partially online in both the Army and Army Reserve.

There is a fine line for the DF to walk. Rigid enforcement or over-formalisation of CPD will deter leaders from pursuing it naturally. It merely becomes a 'box-ticking' exercise where there is little incentive to do more than the minimum required.³¹ When implemented with care, hybrid models offer a genuine opportunity to modernise military education, empower junior leaders, and cultivate a culture of lifelong learning across the force.³²

Recommendations and Conclusion

To meet the demands of the contemporary operating environment, the DF must take proactive steps to integrate informal learning into its professional military education framework. Based on the evidence presented above, several recommendations can be made.

Firstly, the DF should develop a system to recognise and encourage informal learning without over-formalising it. This could take the form of an optional CPD log or digital learning journal, allowing personnel to record learning activities such as podcasts, personal reading, or participation in online military education platforms. To incentivise engagement, personnel who meet annual CPD thresholds could be offered small rewards, such as days in lieu or other appropriate rewards. There are several examples of forms of CPD active in the public service that the DF can draw ideas from. Secondly, blended and modular learning should continue to be expanded across Regular and Reserve training programmes. More courses should be offered in shorter, flexible formats, including online components, particularly for the Reserve Defence Forces whose availability is limited. This has already been recognised in the JPME Strategy. Finally, the DF should consider creating an in-house PME platform similar to *The Cove* or *Line of Sight*.³³ This would provide a trusted environment for informal learning, promote reflection, and encourage knowledge sharing across ranks and roles. It will also provide a loose structure that should ideally counter the risks of unregulated informal learning. These international models offer proven frameworks that the DF can adapt to meet domestic needs.

31 Tom Clark, "Professional Military Education: A Highly Peculiar Missing Link," *Small Wars Journal* (Arizona State University), September 18, 2024, <https://smallwarsjournal.com/2011/05/10/professional-military-education-a-highly-peculiar-missing-link/>.

32 Mark J. Lavin II "Training or Educating: A Choice for Developing the Next Generation of Army Leaders," *Small Wars Journal* (Arizona State University), January 18, 2023, <https://smallwarsjournal.com/2023/01/18/training-or-educating-choice-developing-next-generation-army-leaders/>.

33 Government of Australia, "Evolving an Intellectual Edge."

In conclusion, the rise of informal and decentralised learning reflects a wider cultural shift in how knowledge is accessed and absorbed. Rather than resist this change, the DF should harness it to foster critical thinking, professional curiosity, and lifelong development. By embracing hybrid learning models and informal learning behaviours, the DF can empower its junior leaders to become more adaptive, better informed, and more effective in the complex environments they are expected to lead in. In doing so, it will not only modernise its educational approach but also strengthen its operational capability in an era of constant change. This is a meaningful step toward developing adaptive, resilient, and capable leaders for the future.



Simulating Complexity: Urban Operations, Cognitive Load & Wargaming in the Contemporary Operating Environment

Lieutenant Colonel Brian Cahill

Introduction

The Urban battlespace uniquely tests soldiers' resilience, judgement, and adaptability, now central to the contemporary operating environment. We are witnessing global urban growth on an exponential scale, with approximately 68% of the worldwide population (6.8 billion) is expected to live in urban areas by 2050,¹ growing fastest in the developing world.² This paper will examine the leadership challenges posed by modern urban operations (UOs) and their implications for Irish land force commanders, both in territorial defence and in supporting international military efforts. In addition, it will assess how integrating enhanced decision-making processes and wargaming can improve the Irish Army's operational effectiveness in urban environments whilst mitigating hybrid threats to the land force.

Understanding the Implications of UOs in the Contemporary Operating Environment

Cities have long served as strategic centres of gravity, their political, economic, and social significance making them focal points of war, where outcomes were frequently determined by siege warfare on their peripheries.³ Alex Neads describes this as the “*totemic value of cities*”⁴ and the defeat of an adversary, whether a peer or an asymmetric force, is often linked to the ‘fall’ of the city itself. However, UOs since the end of the twentieth century have demonstrated a marked difference, with operations generally focused on terrain control within the city itself, characterised by prolonged, costly, building-to-building fighting in complex modern urban landscapes.⁵ One can argue that the lesson from Russia's military blunder in Ukraine is not to avoid urban warfare, but to accept its inevitability.⁶ UOs present a formidable challenge across the peace, security, and law enforcement spectrum and can be considered the most physically demanding and resource-intensive form of conventional military operations.⁷

Clausewitz's ‘remarkable trinity’⁸ is most vividly realised in urban warfare, where the interplay of passion, chance, and reason is intensified as political authority, military operations, and civilian populations converge within a compressed battlespace.⁹ The importance of achieving harmony between the grand strategic and tactical levels is

1 United Nations Dept. of Economic and Social Affairs, *World Social Report 2022: Inequality in a Rapidly Changing World*, (New York: United Nations, 2022).

2 2% per Annum. World Bank - *Urban Development* (2024) accessed 15 Sep 25. <https://www.worldbank.org/en/topic/urban-development/overview>

3 For example, the 23 sieges of Jerusalem, Constantinople in 1453 and Vienna in 1683.

4 Alex Neads, “The Totemic Value of Cities,” in: L. Turchewics, ed., *Small Armies, Big Cities: Rethinking Urban Warfare*, (Boulder: Lynne Rienner, 2022), 52.

5 Aachen, Stalingrad, Aleppo, Mosul, and Bakhmut.

6 Margarita Konaev and Kirstin Brathwaite, “Russia's Urban Warfare Predictably Struggles,” *Foreign Policy* April 4, 2022. Accessed 15 Sep 25. <https://foreignpolicy.com/2022/04/04/russia-ukraine-urban-warfare-kyiv-mariupol/>

7 Margaret Williams and Max Cheng, *The Future of Urban Warfare*, 2023. Irregular Warfare Initiative. Accessed 01 Aug 25. <https://irregularwarfare.org/articles/the-future-of-urban-warfare/>

8 Edward Villacres and Christopher Bassford, “Reclaiming the Clausewitzian Trinity,” *Parameters* 25 no.1(1995): 9.

9 The people, the Military & the Government - while useful as a simplification, this abstraction must be used with caution—it risks masking the deeply institutional and sociopolitical forces Clausewitz saw as shaping war's conduct and evolution.

especially critical in modern UOs, where civilian populations, military personnel, and strategic objectives converge in densely populated areas.¹⁰ More recently, these observations have been supported by a wide range of academics,¹¹ who all agree that the complexities of urbanisation increase the likelihood that at least some conflict will occur in urban centres¹² and is therefore an operational reality that must be reflected in both Irish Army training and doctrine, irrespective of the scale of our forces or traditional expeditionary posture. Urban operations constitute a 360-degree threat environment, with canalised movement corridors, restricted manoeuvre space, and compressed weapons engagement ranges. Furthermore, different physical structures yield drastically different weapon effects on targets, limiting a commander's tactical options.¹³ It also has a clear impact on the traditional IPB¹⁴ process, where 2D terrain analysis often falls short of accounting for the 3D nature of the operating environment (Fig. 1).

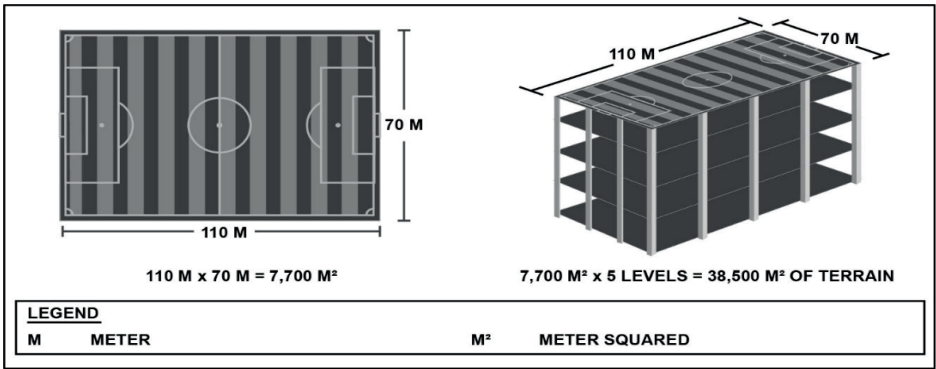


Fig. 1 – Urban Environment Surface Area¹⁵

Indeed, urban environments undergo rapid alterations due to heavy fighting, where buildings are rubblised, road networks change, new openings appear¹⁶ and obstacles suddenly arise as infrastructure degrades. Different urban terrain zones (UTZs) exhibit distinct physical and human characteristics,¹⁷ requiring adaptable force structures and operational concepts specific to the demands of each environment. For example, light

10 John Spencer, "A Clausewitzian Lens on Modern Urban Warfare," *Modern War Institute* (2025). Accessed 01 Aug 25. <https://mwi.westpoint.edu/a-clausewitzian-lens-on-modern-urban-warfare/>

11 Emma Elfversson, "Contentious cities? Urban growth and electoral violence in Africa," *World Development*, 193 no. 1 (2025): 107; Anthony King, *Urban Warfare in the Twenty-First Century* (London: Polity, 2022); Gian Gentile, David Johnson, Lisa Saum-Manning, Raphael Cohen and James Doty III, *Reimagining the Character of Urban Operations for the U.S. Army: How the past Can Inform the Present and Future* (Santa Monica, Calif.: Rand Corporation 2017).

12 Urban centres are defined as settlements of at least 50,000 inhabitants with greater than 1,500 inhabitants per sq. km; towns and urban clusters are defined as areas with at least 5,000 inhabitants and a density of at least 300 inhabitants per sq. km; and suburban or peri-urban areas are those urban areas which fall outside the contiguous area of an urban cluster. *EUROSTAT*, "Applying the Degree of Urbanisation -a Methodological Manual to Define Cities, Towns and Rural Areas for International Comparisons 2021 Edition". <https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/ks-02-20-499>.

13 Mosul Study Group, *What the Battle for Mosul Teaches the Force*, (Fort Leavenworth: TRADOC, September 2017), 30–31). <https://www.armyupress.army.mil/Portals/7/Primer-on-Urban-Operation/Documents/Mosul-Public-Release1.pdf>.

14 Intelligence Preparation of the Battlespace – broken into four stages – Define the Battlespace Environment, describe the battlespace effects, evaluate the threat and determine Courses of Action (COAs).

15 US Army, *Bde Combat Team manual ATP 3.06-11*, (Fort Leavenworth: TRADOC, 2024), 7. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN42031-ATP_3-06.11-000-WEB-2.pdf

16 For entry/exit/firing.

17 NATO doctrine identifies 8 zones – Historical centre/old town, financial/business centre, heavy industrial area, light industrial area, high density residential, low density residential, slum/shanty areas & subterranean. NATO, *ATP-99 Urban Tactics* (Brussels: NATO Standardization Office, 2017), p2-3.

forces excel in historical the ‘old city’, while heavy armoured forces are better suited for industrial areas with more manoeuvre space and long sight lines for weapons systems.¹⁸ Furthermore, the presence of civilians imposes constraints on military actions that are often less significant in rural fighting.¹⁹

From a national defence perspective, over the last twelve years, the urbanisation trend has been evident in Ireland, where six urban areas meet the requirements for urban centre classification,²⁰ with approximately 37% of the population living within them. In addition, 25% of the population live in towns and urban clusters.²¹ Brigadier Ian Rigden highlights that land forces have struggled to update their doctrine, creating a training gap for most Western forces and failing to adequately address challenges to force sustainment, force protection, and the protection of civilians. He states:

Modern urban conflict is congested, contested, connected, and constrained... fought among the people in an artificial environment, it poses unique challenges. Rarely does it produce clear winners, calling into question traditional notions of victory.²²

While there is a clear need to develop non-kinetic capabilities to address the threat environment across the electronic spectrum and the cyber domain, land forces, of all sizes, will always remain necessary to secure terrain and defeat opponents in close battle.²³ As stated by former UK Chief of the General Staff General Sir Patrick Sanders²⁴ at a RUSI Land Power conference in 2022, “you can’t cyber your way across a river.”²⁵ Consequently, there exists a requirement for all commanders to be trained to be adaptable in confused C4i²⁶ scenarios and exercise their rapid military decision-making skills.

18 Stuart Lyle, The Role of Wargaming in Urban Operations Training, *The Canadian Army Journal*, Oct (2021-1), 36. <https://www.canada.ca/en/army/services/canadian-army-journal/articles/2024/21-1-lyle-wargaming-in-urban-ops-training.html>

19 ICRC, “Reducing Civilian Harm in Urban Warfare: A Commander’s Handbook,” (ICRC, November 2021), <https://www.icrc.org/en/document/reducing-civilian-harm-urban-warfare-commanders-handbook>.

20 Dublin, Cork, Limerick, Galway, Waterford & Drogheda.

21 Central Statistics Office (2023). Population Distribution - CSO - Central Statistics Office. www.cso.ie/en/releasesandpublications/ep/p-cp2tc/cp2pdm/pd/

22 Ian Rigden, “The Poisoned Chalice: Urban Warfare in the Twenty-First Century and beyond,” in: G. Fremont-Barnes, ed., *A History of Modern Urban Operations*, (London, Palgrave Macmillan, 2022), 346; Gordon Paendleton, G., “New Concepts - Joint Urban Operations and the NATO Urbanisation Project,” Dec 2015.

23 Conor Gallagher, “State to Be Advised to Establish Military Cyber Command,” *The Irish Times*, 31 Jan 2022. www.irishtimes.com/news/ireland/irish-news/state-to-be-advised-to-establish-military-cyber-command-1.4789385

24 Gen. Sir Patrick Sanders, *Chief of the General Staff Speech at RUSI Land Warfare Conference*, speech, Church House, Westminster, June 28, 2022, Gov.uk. www.gov.uk/government/speeches/chief-the-general-staff-speech-at-rusi-land-warfare-conference

25 Or in this case, get a platoon across a road, junction, through a city block, occupy a rooftop etc.

26 Command & Control, Communication, Computers, and Intelligence

The Case for Urban Educational Wargaming

A special relationship between war and games has always existed, dating back to the enactment of ancient spectacles and the playing of strategic board games.²⁷ This historical context is crucial to understanding the evolution of wargaming. Indeed, “*ever since words existed for fighting and playing, men have been wont to call war a game.*”²⁸ The utility of the modern war game was investigated and expanded by the Prussians, whose development of the Kriegsspiel provided commanders with a new way to practice tactics and develop strategies to counter potential opponents’ strengths.

Wargaming lacks a single definition, though scholars agree on its training value and cognitive development. Several scholars have focused on the role and use of serious games/simulations²⁹ as well as the broader use of wargaming in an educational setting.³⁰ However, this paper will specifically analyse mechanical wargaming, a unique form of gaming where physical pieces are used on a board/map as a development and training tool for professional military training. To guide this exploration, Peter Perla’s 1990 definition of wargaming is the most suitable: “*A warfare model or simulation in which the flow of events shapes, and is shaped by, decisions made by a human player or players during the course of those events.*”³¹ Wargaming, when correctly applied, could be of significant value to the Irish Army’s decision-making and UOs training when applied and run correctly.³² The last ten years have seen a renaissance in mechanical wargaming,³³ with its value notably recognised by the USA, the UK, and China.³⁴ While the Irish Army lacks the physical urban training areas of suitable scale to execute unit-level exercises, wargaming can fill the gap that the Commandant of the USMC called in 2019 “*arguably our greatest deficiency in the training and education of leaders: practice in decision-making against a thinking enemy.*”³⁵ The British Army is equally enthused about the utility of wargaming, having conducted the largest force development wargame in living memory in late 2023.³⁶

27 Max Nelson, “Battling on Boards: The Ancient Greek War Games of Ship Battle (Naumachia) and City-State (Polis),” *Mouseion* 17, no. 1 (2020): 3–42.

28 Johan Huizinga 1970, 110; cited in Philip Sabin, *Simulating War: Studying Conflict through Simulation Games*, (London: Bloomsbury Academic, 2019), 16.

29 Anja Van Der Hulst, Tijmen Muller, Sam Besselink, and Nathalie Tno. “The Potential of Serious Games for Training of Urban Operations.” NATO JWC 2019. <https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-111/MP-MSG-111-19.pdf>.

30 Amanda Rosen and Lisa Kerr, “Wargaming for Learning: How Educational Gaming Supports Student Learning and Perspectives,” *Journal of Political Science Education* 20, no. 2 (2024), 319; Kenneth O’Rourke, “Is the Irish Defence Forces Playing It Safe with Experiential Learning? Exploring the Risks and Opportunities of Adversarial Educational Wargaming in Irish Defence Forces Intermediate Professional Military Education,” (MA thesis, SETU, 2023); Karsten Bräthen, Ole Mevassvik and Rikke Seehuus, *Simulation Support to Wargaming for Tactical Operations Planning*. In: C. Turnitsa, C. Blais and A. Tolik, eds., *Simulation and Wargaming* (New Jersey: Wiley, 2024), 225.

31 Peter Perla, *The Art of Wargaming: a Guide for Professionals and Hobbyists* (Annapolis: Naval Institute Press, 1990), 164.

32 Eric Walters, “Wargaming in Professional Military Education: Challenges and Solutions,” *Journal of Advanced Military Studies* 12 no. 2 (2021), 81. www.muse.jhu.edu/article/805919.

33 Aggie Hirst, “States of play: Evaluating the Renaissance in US Military Wargaming,” *Critical Military Studies* 8 no. 1 (2022), 3.

34 Burak Yuksek, Guney Guner, Hasan Karali, Batu Candan, and Gokhan Inalhan, “Intelligent Wargaming Approach to Increase Course of Action Effectiveness in Military Operations,” *AIAA 2023-2531* (AIAA SciTech Forum 2023, National Harbor, MD, January 23–27, 2023), 3.

35 USMC - 38th Commandant’s Planning Guidance CPG, (2019), 19. Accessed 12 Aug 25. www.marines.mil/News/Publications/MCPPEL/Electronic-Library-Display/Article/1907265/38th-commandants-planning-guidance-cpg/

36 Nick English and Paul Elrick, “Casting Aside the Crystal Ball- Placing Wargaming at the Heart of Force Design,” *British Army Review*, (Autumn 2023), 20. https://issuu.com/chacr_camberley/docs/185; Tom Lamont, “What Would Happen If Russia Invaded Finland? I Went to a Giant War Game in London to Find out,” *The Guardian*, 30 Sep 23. www.theguardian.com/politics/2023/sep/30/what-would-happen-if-russia-invaded-finland-i-went-to-a-giant-war-game-in-london-to-find-out

Since terrain and inhabitants are crucial factors in UOs, simulating these chaotic variables to produce a realistic training environment has always been difficult for armies during peacetime training.³⁷ However, using wargaming as a tool, the Irish Army could facilitate participants to think critically about the impact the physical and human terrain can have on a force conducting UOs within its means and capabilities.³⁸ It is essential to note that wargaming is not a panacea for a force's doctrinal and training shortcomings. It can even be detrimental if the models and concepts used do not reflect the realities of the conflict.³⁹ Knowing when NOT to wargame a scenario is equally as important, especially if there is a risk of 'Game washing' where the wargame is being used to prove a concept or doctrine or increase the chances of it being adopted.⁴⁰

Cognitive Load and Urban Command: Theoretical Foundations

One of the principal challenges of future urban warfare is the exponential increase in cognitive load experienced by commanders and decision-makers, driven by dense information flows, compressed time horizons, and complex physical terrain and human factors. Several research projects⁴¹ have found an increased cognitive burden on junior commanders in complex urban operating environments as opposed to a traditional rural setting. Therefore, it is crucial to examine how commanders are likely to think and how the urban environment impacts their heuristics. Daniel Kahneman divides the mind into two systems.⁴² 'System 1' is fast and intuitive; 'system 2' is slow and effortful, and wargaming can strengthen a commander's ability to shift between them. If we accept this hypothesis, wargaming as a decision-making tool can assist commanders in developing and improving cognitive processing systems and pathways. Indeed, wargaming exemplifies Eisenhower's theory that "Plans are worthless, planning everything".⁴³ Wargaming provides an "intellectually liberating, safe-to-fail environment"⁴⁴, which allows participants to explore the pros and cons of various TTPs and doctrinal approaches in the urban environment at a relatively low cost.

Herbert Simon's bounded rationality⁴⁵ challenges the classical idea that decision-makers are perfectly rational optimisers.⁴⁶ However, especially in urban operations, commanders

37 Harrison Brewer, "Modelling Urban Warfare: How Can We Model the Complexity of Urban Space?" *Georgetown University Wargaming Society*, 08 May 2025. www.youtube.com/watch?v=9mVRg9u7zaw

38 David Burden, "On Wargaming Urban Conflict," *History of Wargaming Project*, 5 September 2025, <https://www.youtube.com/watch?v=MzeaNG1vt9c>

39 Rex Brynen, "Wargaming Doesn't Work. (PAXsims, 2023). Accessed 15 Sep 25. <https://paxsims.wordpress.com/2023/12/17/wargaming-doesnt-work/>

40 Graham Longley-Brown, *Successful Professional Wargames: a practitioner's Handbook*. (London, History of Wargaming Project, 2019), 26.

41 UK Ministry of Defence, "British Army Experiments with Dstl Study on Urban Combat". (GOV.UK, 2023). Accessed on 12 Sep 25. www.gov.uk/government/news/british-army-experiments-with-dstl-study-on-urban-combat; USMC – "Marine Corps Warfighting Lab Experiments with Urban Combat Concepts" (2023). Accessed on 15 Sep 25. www.mcwl.marines.mil/www.mcwl.marines.mil/Divisions/Experiment/AWE/video/705206/

42 Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 45.

43 Angel Contreras, Martine Ceberio, and Vladik Kreinovich, "Plans Are Worthless but Planning Is Everything: A Theoretical Explanation of Eisenhower's Observation." In *Decision Making under Constraints*, edited by Martine Ceberio and Vladik Kreinovich (Chambers: Springer International Publishing, 2020), 93.

44 UK Ministry of Defence, *Wargaming Handbook* (Shrivenham: The Development, Concepts and Doctrine Centre, 2017), 6. https://assets.publishing.service.gov.uk/media/5a82e90d40f0b6230269d575/doctrine_uk_wargaming_handbook.pdf

45 Herbert Simon, "Rational Choice and the Structure of the Environment." *Psychological Review* 63 (2) (1956): 129.

46 Heinz Kurz, "Von Neumann's Growth Model and the 'Classical' Tradition." In *Understanding Classical Economics - Studies in Longperiod Theory*, ed. by Heinz Kurz and Neri Salvadori. London: Routledge, 1998).

rarely have unlimited information, time, or cognitive resources; instead, they must make 'good-enough' decisions under pressure.⁴⁷ His model emphasises making logical decisions while considering the cognitive constraints of the decision-maker, including limitations in knowledge and capabilities.⁴⁸ He outlines that many decision-makers – in this case, military commanders – eventually encounter a situation in which an excessive⁴⁹ amount of information leads to an unfavourable conclusion.⁵⁰ Roetzel visualised overload as an inverted U-curve (Fig. 2).⁵¹ The Y-axis represents the level of decision-making performance. The X-axis denotes the quantity of information or information load, and an individual's optimal decision is at the highest point of the inverted U-curve.

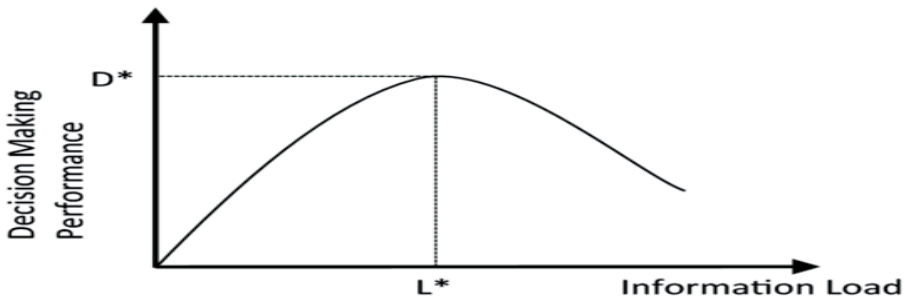


Figure 3.1 Inverted U, Information Overload Relationship to Decision-making
(Roetzel, 2018; p.6)

Fig 2 – Roetzel's cognitive overload graph

Roetzel's definition⁵² of information overload is when a decision-maker is presented with a collection of data comprising many informational signals of varying size and complexity. This abundance of information hampers the decision-maker's capacity to make the best possible decision efficiently. Klingberg⁵³ and Miller⁵⁴ add that the average human working memory has an inherent limitation, allowing us to retain approximately seven items of information.⁵⁵ If we accept the findings, it is evident how they will impact the commander's cognitive computational abilities in the urban environment.⁵⁶

UOs create a barrage of stimuli, from the noise of city life to the increased acoustic impact of gunfire. The presence of buildings can negatively impact GPS, radio signals and UAV

47 Herbert Simon, *Models of man; Social and rational*, (New Jersey: Wiley, 1957); Herbert Simon, (1990). Bounded Rationality. In: J. Eatwell, M. Milgate and P. Newman, eds., *Utility and Probability* (London: Palgrave Macmillan UK, 1990) p15–18.

48 Simon, *Bounded Rationality*, 15.

49 Or indeed the opposite – incomplete or conflicting information

50 Brandon Doggette, *Information overload: Impacts of Brigade Combat Team s-2 Current Operations Intelligence Analysts*. (MA Thesis, 2020). Accessed on 12 Sep 25. <https://apps.dtic.mil/sti/pdfs/AD1124624.pdf>

51 Peter Roetzel, "Information Overload in the Information age: a Review of the Literature from Business administration, Business psychology, and Related Disciplines with a Bibliometric Approach and Framework Development". *Business Research*, 12 (2) (2018).

52 Roetzel, "Information Overload in the Information age", 16

53 Torkel Klingberg, *The Overflowing Brain: Information Overload and the Limits of Working Memory*, (New York: Oxford University Press, 2009).

54 George Miller, "The Magical Number seven, plus or minus two: Some Limits on Our Capacity for processing information". *Psychological Review*, 63, 81.

55 Miller, "The Magical Number seven, plus or minus two: Some Limits on Our Capacity for Processing information", 85

56 Klingberg, *The Overflowing Brain*, 55, cited in Doggette, *Information Overload*, 17

support.⁵⁷ The operating picture can change rapidly, with buildings and neighbourhoods changing hands and ground routes being destroyed or blocked.⁵⁸ Commanders in UOs face high-stakes, ambiguous decisions; the risk of civilian casualties from urban fires is much higher.⁵⁹ In this grey area, the potential negative consequences of inaction can outweigh the risk of choosing a solution that is not perfect but satisfactory.⁶⁰ Mechanical wargaming can provide a valuable means of simulating information limitations and time constraints, artificially challenging the commander to reassess whether their selected course of action is still achieving its objectives as the scenario develops. This prepares commanders to operate within practical constraints, making quick, satisfactory judgments and identifying situations that require additional information.⁶¹

Wargames can be highly effective when specifically created to replicate situations involving limited situational awareness. This entails limiting the dissemination of intelligence, imposing time constraints, and introducing external actor actions, all of which compel players to manage the consequences of their decisions.⁶² Games that centre on a sequence of interrelated decisions highlight that settling for something satisfactory in the present may yield unforeseen consequences in the future. As Simon⁶³ outlined in a fundamental tenet of his bounded rationality theory, this is known as “satisficing”.⁶⁴ Satisficing recognises the limitations of real-world decision-making and involves setting a minimum acceptable threshold⁶⁵ and selecting the first solution that meets or exceeds it, i.e., what is good enough to achieve the task. It may not be the best solution in a hypothetical world, but it is achievable for the given situation, resources, and time.⁶⁶ Wargaming facilitates the development of the Satisficing skills of commanders and improves their capacity to adjust and respond effectively to new or changing circumstances.

The second model to be examined is the Prospect theory proposed by Kahneman and Tversky.⁶⁷ Their model posits that individuals (commanders) make choices under risk, not on an absolute outcome basis but relative to a reference point. *Traditional risk models, rooted in games of chance,* ⁶⁸ *prescribe ideal decisions but fail to reflect how commanders truly think under pressure.* Prospect theory consists of two stages. In the first or editing stage, outcomes and contingencies are framed, and extremes⁶⁹ are discarded or solidified. The second stage

57 Oguz Isik, Juhyeon Hong, Ivan Petrunin, and Antonios Tsourdos, “Integrity Analysis for GPS Based Navigation of UAVs in Urban Environment.” *Robotics* 9 (3) (2020), 66.

58 Widlore Mérancourt and Samantha Schmidt, “As Gangs Attack a Critical port, ‘Haiti Will Go Hungry Soon’.” *Washington Post*, (07 Mar 2024). www.washingtonpost.com/world/2024/03/07/haiti-gangs-port/

59 ICRC, “New Research Shows Urban Warfare 8 Times More Deadly for Civilians in Syria and Iraq”, (01 Oct 2018) International Committee of the Red Cross. www.icrc.org/en/document/new-research-shows-urban-warfare-eight-times-more-deadly-civilians-syria-iraq

60 Over-analysis and indecision

61 Sarah Fisher and David Mandel, “Teaching & Learning Guide for: Risky-choice Framing and Rational Decision-making”. *Philosophy Compass*, 16 (12), (2021). 12.

62 unintended or otherwise - The impact of these consequences can then be assessed through follow on ‘Green Team’ analysis

63 Simon, “Rational Choice and the Structure of the environment”, 130

64 Simon, “Rational Choice and the Structure of the environment”, 131

65 specified mission task

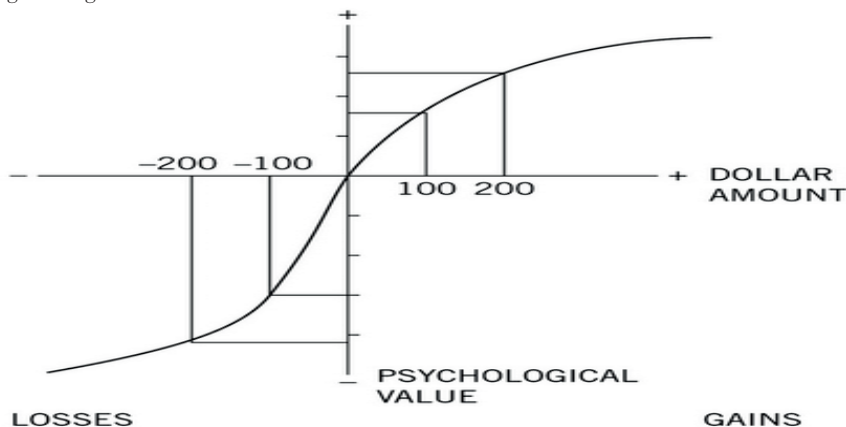
66 Florian Artinger, Gerd Gigerenzer, and Perke Jacobs. “Satisficing: Integrating Two Traditions.” *Journal of Economic Literature* 60 (2) (2022), 598.

67 Kahneman, *Thinking, Fast and Slow*, 48; Kahneman, Daniel, and Amos Tversky. “Prospect Theory: An Analysis of Decision under Risk.” *Econometrica* 47 (2) (1979), 263.

68 James Schultz, *Military Decision Making and Prospect Theory. A Framework for Military Decision Making under Risks*, (Colorado, Air University Press, 1997) 5.

69 i.e. likely/unlikely events

consists of assessing the available options based on the subjective value assigned to each outcome and choosing a course of action. During this phase, the commander's "domain of reference" is established.⁷⁰ Kahneman and Tversky⁷¹ propose that commanders fall into two reference domains. The first is a 'gains domain', where commanders are generally risk-averse when choices are framed as potential gains. They prefer certainty to the chance of even greater gains. The second is a 'loss domain' where commanders become risk-seeking



when faced with potential losses, willing to gamble on risky options that might mitigate or offset the loss.

Fig. 3 – Kahneman's Loss Aversion Model

In UOs, negatively framed reference points⁷² can push commanders into the 'loss domain', prompting risky behaviour.⁷³ even if it jeopardises mission accomplishment. The theory, coined by Kahneman as "loss aversion" (Fig.3)⁷⁴, posits that people respond to losses more acutely than to a similar gain - "losing hurts more than a comparable gain pleases"⁷⁵ and that "losses loom larger than gains".⁷⁶ Conversely, if their objective seems out of reach and mission failure is looming, commanders may be compelled to act more recklessly and take gambles or launch a forlorn hope for a chance of a last-minute reversal of fortunes. UOs, regardless of where on the conflict scale they occur, are confusing and unpredictable, which can lead urban commanders to take high-risk, often unnecessary measures to create a sense of control over a seemingly lost situation. According to prospect theory, the overestimation of low-probability events can also be observed when people seek gains. Poorly trained commanders can overestimate the likelihood of attaining a high-value objective, even when the probability of success is very low.⁷⁷ This overestimation of low-probability events can encourage commanders to make irrational decisions when considering the odds and the gap between expected value and costs. Notwithstanding the unique context, this

70 Adam Biggs and Kyle Pettijohn, "Prospect Theory and Its Implications for Adversarial Decision-making". *The Journal of Defense Modelling and Simulation: Applications, Methodology, Technology*, 18(2) (2019), 1.

71 Tversky, "Prospect Theory: An Analysis of Decision under Risk", 269.

72 i.e. losing troops, civilian casualties, losing control of terrain and mission failure

73 Schultz, *Military Decision Making and Prospect Theory*, 10.

74 Kahneman, *Thinking, Fast and Slow*, 42.

75 Schultz, *Military Decision Making and Prospect Theory*, 12.

76 Kahneman, 46 – simply, he showed that some people feel that loosing \$100 feels worse than winning \$200 feels good

77 Kahneman, *Thinking, Fast and Slow*, 463

was likely a contributing factor in the relentless counterattacks launched by mercenaries of the Wagner Group in Bakhmut from May 2022 to May 2023, losing an estimated twenty thousand fighters despite Ukrainian territorial gains and the Russian government's operational focus shifting away from the city.⁷⁸

Wargaming can be used to explore how choice 'framing' influences decision-making, as described in Prospect Theory. By changing how a mission is worded, a scenario can subtly shift a commander's reference point. For example, a task might be framed in the gain domain ("*Secure Building X to gain a tactical advantage*") or in the loss domain ("*Do not lose Building X*").⁷⁹ How participants respond to these different framings can reveal biases in their decision-making processes.⁸⁰ Finally, wargaming AARs⁸¹ can assist commanders in identifying where they might be falling for a framing effect and in making overly risky or cautious decisions, all within a non-kinetic, safe-to-fail-and-learn environment⁸². The following section will examine how wargaming can be used by the Irish Army to develop the cognitive skills outlined above and to practice applying doctrine and TTPs when physical training areas are unavailable or unsuitable.

The Challenge: Wargaming to Train Better Decision-Makers

Simulating the complexity of urban operations (UOs) in wargames remains a significant challenge. As Prof. Philip Sabin observes, it is often an issue of force-to-space ratio.⁸³ For example, when you look at the Bn strength force that occupied the area in the vicinity of Arnhem Bridge in September 1944, they occupied an area just 300m²⁸⁴, a tiny part of any hex-style game board. A US Army review of legacy simulation tools assessed across the PMESIL-PT⁸⁵ framework, found that only the "Military" component rated green⁸⁶—highlighting the limitations of existing models in capturing the multidimensional nature of urban warfare. Nevertheless, wargaming is not a universal solution. As commonly stated among simulation experts, "all models are wrong, but some are useful."⁸⁷ No wargame can capture the totality of reality; they are necessarily reductive. The utility lies in identifying the level of fidelity required for a given training outcome and accepting abstraction where it supports the primary aim. Wargames intentionally focus on particular dynamics while abstracting others—combat resolution with dice, for example, represents not just randomness but the friction and uncertainty inherent to real-world conflict. Effective wargames do not attempt total realism, but rather create plausible scenarios that compel commanders to grapple with uncertainty, ambiguity, and the cognitive burden of urban command. Used correctly, they

78 Colin Clark, "Bad Company: Wagner Group and Prigozhin at Crossroads in Ukraine". *Foreign Policy Research Institute*, June 23, 2023. <https://www.fpri.org/article/2023/06/bad-company-wagner-group-and-prigozhin-at-crossroads-in-ukraine/>.

79 e.g. failure to secure building X may lead to mission failure

80 Longley-Brown, *Successful Professional Wargames: a practitioner's Handbook*, 300.

81 After Action Reviews

82 Gareth Jones, "Wargame Skills and Learning Analysis for UK MoD Strategic Command", Vedette Consultancy, Oct 2024. Accessed 16 Sep 25. <https://www.professionalwargaming.co.uk/24GarethJonesWargameSkills.pdf>.

83 Sabin, *Simulating War: Studying Conflict through Simulation Games*, 220.

84 Martin Middlebrook, *Arnhem 1944* (London, Routledge, 2019), 126.

85 Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time

86 Lyle, "The Role of Wargaming in Urban Operations Training", 42

87 George Box, "*An Accidental Statistician: the Life and Memories of George E. P. Box*." (Hoboken (Nj): Wiley, 2013) 54.

become valuable cognitive training tools—offering decision-making practice in a safe-to-fail environment and fostering adaptability in complex urban contexts.

Training/learning wargames, or “*fitness programmes for thinking*,”⁸⁸ enable conceptual practice in the real-life concepts of command and control. These games are not the sole creation of military training institutions; commercial games are an excellent source of training materials that can simulate the increased cognitive load and uncertainty associated with UOs. In addition, it can be rolled out as a standalone workshop-style event, run periodically, where doctrine can be discussed in a lecture and a syndicate-style forum as part of continued professional development for both PME students and unit-level training.⁸⁹ This practice would diversify and develop staff officers’ analytical skills as part of doctrinal COA development wargaming.⁹⁰

In an era where conflict is increasingly fought among dense populations, the ability of small, professional forces like the Irish Army to adapt cognitively and tactically to urban operations will be decisive. The growing urbanisation of Ireland, where over 60% of the population now resides in urban centres or clusters, demands that we train not just for expeditionary deployments, but for territorial defence scenarios that could emerge in any town or city across the State. Yet without access to sophisticated urban training facilities or extensive simulation infrastructure, the Irish Army must innovate. Mechanical wargaming offers a uniquely scalable, low-cost, and intellectually demanding training tool to replicate the complexity of urban terrain and the psychological strain it imposes on commanders. While professional wargames are invaluable training, they are not a panacea and do not replace the rigours of real-time exercises and operations. Live training remains essential for the army, but wargaming complements it by preparing commanders at all levels for complex decision-making under pressure and by encouraging tactical adaptability based on available information.

This will not only help prepare commanders at every level to better handle the complex cognitive load in a risk-free environment, but also provide excellent preparation for those who may deploy on exercises in towns and villages across the country. Wargaming needs to be formalised and embedded into the Professional Military Education continuum—from junior NCO training through to the Joint Command & Staff Course, not just for COA development and the synchronisation of actions, but to develop more adaptive, reflective leaders capable of navigating ambiguity, synchronising effects, and making timely decisions under pressure. Future adversaries will opt to fight in an urban environment, and the only way to mitigate this inevitability is through readiness—an imperative, not an option. We must start gaming the last place they want to be—and the first place future conflict will drag them into: the City.

88 Sharpe, 2013, cited in Longley-Brown, 2019, 18

89 Warlord Games Bolt Action for low level PI actions, Sebastian Bae’s Littoral Commander for Joint Operations, We Are Coming, Nineveh! for UOs are excellent examples of what are available commercially

90 Course of Action



From the Epoch of Total Lies to the Epoch of Total Distrust: Leadership Challenges and Doctrinal Shifts in Contemporary Hybrid Warfare

Zurab Bezhanishvili

Introduction: From the Epoch of Total Lies to the Epoch of Total Distrust

We are undergoing a profound transformation in the global security landscape—less defined by conventional warfare and more by the collapse of shared truths. Modern conflict has shifted into the cognitive domain, where perception, belief, and trust are now contested terrain.¹ This article argues that we have moved from an “Epoch of Total Lies,” marked by organized disinformation, into an “Epoch of Total Distrust,” or “The Post-Truth Era,”² where the aim is to fragment societies, delegitimise leadership, and erode epistemic foundations. Ultimately, the battle for trust will define the conflicts of the 21st century. Hybrid warfare has evolved beyond the fusion of conventional and irregular tactics³ into a permanent “Gray Zone condition,” where distinctions between war and peace, truth, and fiction, are increasingly blurred.⁴ Traditional doctrines are being destabilised by AI-driven influence operations, Deep Fakes, and social media manipulation.⁵ As Frank Hoffman noted, hybrid warfare exploits seams in open societies—not just through force, but through manipulation of legitimacy and perception, often remaining below the legal threshold of war.⁶ In the “Epoch of Total Lies,” disinformation was centrally deployed by authoritarian institutions—states, parties, religious groups⁷—to control narratives and justify proxy wars or interventions. From Nazi propaganda to Cold War psyops, lies were institutional and hierarchical. But with the rise of globalisation, digital networks, and interconnected societies, the efficacy of systemic deception began to collapse. Real-time verification, open-source intelligence, and digital accountability have made lies harder to sustain.⁸ Publics have become more cognitively resilient, equipped with tools to challenge falsehoods. However, truth’s decline in centrality—as noted by thinkers like Lee McIntyre⁹—has not produced clarity. Instead, it has given rise to epistemic fragmentation:¹⁰ polarised realities, algorithmic amplification, and societal confusion. Today, distrust itself is the strategy.¹¹ The goal is no longer to assert a false truth, but to destroy the credibility of all narratives—producing paralysis, delegitimation, and cognitive exhaustion.¹² Contemporary geopolitical competition has shifted toward non-kinetic domains, emphasizing information warfare and soft power. As Lind observes, “new autocracies do not rely solely on repression,” but instead deploy “smart

1 Laurie Fenstermacher, David Uzcha, Katie Larson, Christine Vitiello, and Steve Shellman, “New Perspectives on Cognitive Warfare,” *Signal Processing, Sensor/Information Fusion, and Target Recognition XXXII*, vol. 12547 (14 June 2023): 175

2 Simona Modreanu, “The Post-Truth Era?” *Human and Social Studies* 6 (2017): 7–9.

3 James Kenneth Wither, “Making Sense of Hybrid Warfare,” *Connections: The Quarterly Journal* 15 (2016): 78

4 Vladimir Andrassy and Martin Ondruš, “The Gray Zone and Its Place in Security Environment,” *Challenges to National Defence in Contemporary Geopolitical Situation* 1, no. 1 (2024): 92–93

5 Jahara Matisek and Buddhika Jayamaha, *Old and New Battlespaces: Society, Military Power, and War* (Boulder: Lynne Rienner Publishers, 2022): 68 <https://doi.org/10.1515/9781955055079>

6 Frank Hoffman, as referenced in Colonel Steven C. Williamson, *From Fourth Generation Warfare to Hybrid War* (U.S. Army War College, 2009). 5–6 <https://apps.dtic.mil/sti/tr/pdf/ADA498391.pdf>

7 Marcin Składanowski, Andrzej Szabaciuk, and Agnieszka Łukasik-Turecka, “Church of War: Propaganda and Disinformation in Patriarch Kirill’s Discourse on Russia’s Aggression,” *Cogent Arts & Humanities* 12, no. 1 (2025), 6 <https://doi.org/10.1080/23311983.2025.2515329>

8 Damien Van Puyvelde and Fernando Tabárez Rienzi, “The Rise of Open-Source Intelligence,” *European Journal of International Security*, 2025, 7–8

9 Pavol Hardoš, review of “Post-Truth”, by Lee McIntyre, *Organon F* 26, no. 2 (2019): 311 DOI:10.31577/orgf.2019.26210.

10 Tudor Cosmin Ciocan, “The Ends of Certainty. From Singular Truth to Informational Noise: Rethinking Knowledge in a Fragmented World,” *DIALOGO*, 2025: 248–249 <https://doi.org/10.51917/dialogo.2025.11.2.17>

11 Ruth Mayo, “Cognition Is a Matter of Trust: Distrust Tunes Cognitive Processes,” *European Review of Social Psychology* 26, no. 1 (2015): 288

12 Martin Crilly “Prosecuting the Post-Digital Hyper-War.” *The RUSI Journal* 167 (2022): 79–80.

authoritarianism,” blending coercion with competence and selective openness.¹³ The growing socio-economic and technological complexity undermines traditional centralized authoritarianism, prompting hybrid governance models that integrate central control with decentralized, technologically enabled administration.¹⁴ The rise of digital technologies, global education, and a fact-based epistemic culture¹⁵—the emergence of a “cognitive society”¹⁶—has weakened the efficacy of systemic deception while introducing novel challenges. Two primary drivers underpin this shift: dominant powers’ aversion to large-scale war and the transformation of publics into information nodes.¹⁷ Economic interdependence and technological integration expose societies to external influence, rendering trust a critical vulnerability. In this “Epoch of Total Distrust,” truth loses mobilizing power as pervasive suspicion undermines communication, legitimacy, and institutional stability. Militarily, advanced technologies—combined with evolving sociopolitical and international dynamics—undermine defense systems by disrupting command structures, impairing decision-making, and weakening unit cohesion, thereby requiring new leadership approaches and skill sets.¹⁸

Three Operational Realities Require Attention of Military Leadership:

1. “Digital Stratification”: A digitally literate minority coexists with a majority that remains vulnerable to traditional manipulation due to limited digital and media literacy.¹⁹ It should be noted that the digitally aware population is also losing its resilience due to the modernization of new manipulation techniques.
2. “Obsolescence of Traditional Propaganda”: The primary threat today is no longer the big lie, but rather “total distrust”—a deliberate strategy aimed at eroding belief in any truth and the values.
3. “Systemic Dependence on Technology and Expertise”²⁰: All spheres—socio-cultural, institutional-administrative, global-economic, military-operational, and international—now depend on technology, the availability of high-quality specialists, and the effectiveness of their communication and application.

13 Jennifer Lind, “Authoritarian Adaptation and Great Power Competition” (Washington, DC: Henry A. Kissinger Center for Global Affairs, Johns Hopkins SAIS, August 2023), accessed September 3, 2025, <https://saiss.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/authoritarian-adaptation-great-power-competition>

14 Kostina Prifti et al., eds., “Digital Governance: Confronting the Challenges Posed by Artificial Intelligence”, *Information Technology and Law Series*, vol. 39 (Cham: T. M. C. Asser Press, 2024), 4-5 <https://doi.org/10.1007/978-94-6265-639-0>

15 Johanna Kallio, “The Epistemic Culture of the OECD and Its Agenda for Higher Education,” *Journal of Education Policy* 36, no. 6 (2020): 779–800, <https://doi.org/10.1080/02680939.2020.1745897>

16 Hans-Jörg Trenz, “The theory of the public sphere as a cognitive theory of modern society,” *Philosophy & Social Criticism* 50, no. 1 (2024): 135–136

17 Ilan Manor, “The Chessboard and the Web: Strategies of Connection in a Networked World”, *International Affairs* 94, no. 1 (January 2018): 191–92

18 https://www.nato.int/cps/en/natohq/topics_184303.htm#:~:text=

19 Manuel Castells, “The Network Society Revisited,” *American Behavioral Scientist* 67, no. 7 (2022): 944,

20 Simon Keenan, “Military Decision-Making in an Age of Algorithmic Warfare: Implications for Irish PME,” *Journal of Military History and Defence Studies* 6, no. 3 (2025): 88, <https://ojs.maynoothuniversity.ie/index.php/jmhds/article/view/241>

Doctrinal Shifts in Contemporary Hybrid Warfare: Geopolitical Challenges for Military Leadership

Hybrid warfare has deep historical roots, seen from the Peloponnesian War²¹ to Cold War-era strategies²² blending conventional, covert, and legal tools. In today's context, hybrid doctrines are often split between "offensive" (e.g., Russia, China, the U.S.) and "defensive" (e.g., NATO, EU) models. Professor Ian Easton of the U.S. Naval War College, in his latest research, illustrates how offensive doctrines rely on guile, psychological manipulation, and shock tactics to unbalance defenders. These strategies involve concealing true intentions, staging diversionary feints, and employing advanced technologies such as unmanned amphibious vehicles, containerized missile systems, and AI-driven disinformation.²³ A pivotal doctrinal shift came with Russia's 2008 war in Georgia, later conceptualized through the "Gerasimov Doctrine".²⁴ This approach matured in the 2022 Ukraine invasion, combining information operations, cyberattacks, and military force to reassert regional influence.²⁵ It also targets fragmented populations in the West—marginalized, distrustful, or digitally unaware groups—turning them into channels for influence. These fragmented enclaves, or "monochromatic blotches," mirror tactics previously used in Georgia, Chechnya, and Ukraine. Russia's hybrid strategy unfolds across three gray-zone layers:

1. Internal Gray Zones: Marginalized communities within EU states—ethnic, religious, or ideological groups with low digital literacy—vulnerable to manipulation.²⁶
2. Pro-Russian Weak Links: Political movements, separatist regions, and cultural constituencies with historic or strategic ties to Moscow.
3. Associated Gray-Zone States: Countries such as Hungary, Slovakia, Turkey, Georgia and some others that serve as platforms for logistical and ideological infiltration, predominantly, into the EU.

This model allows for sustained, diffuse pressure on Western institutions through the manipulation of social networks, affiliations, and resentment.²⁷ While the EU has initiated a defensive hybrid doctrine—including the "EEAS Strategic Communication Task Forces",²⁸

21 James Kenneth Wither, "Making Sense of Hybrid Warfare," *Connections: The Quarterly Journal* 15 (2016): 74 DOI:10.11610/Connections.15.2.06

22 Hasan Suzen, "A Comparative Study of 'Russian Political Warfare against the West and the Western (NATO & EU) Counteractions,'" *Horizon Insights (Political & Hybrid Warfare*, January 24, 2018), accessed \August 2, 2025), <https://behorizon.org/russian-political-warfare-against-na-to-eu-counteractions/>

23 Ian Easton, "Foggy with a Chance of Surprise Attack: PLA Amphibious Deception in a Taiwan Scenario", *China Maritime Report*, no. 50 (Newport, RI: China Maritime Studies Institute, U.S. Naval War College, September 23, 2025), <https://digital-commons.usnwc.edu/cmsi-maritime-reports/50>

24 Charles K Bartles, "Getting Gerasimov Right," *Military review* 96 (2016): 30. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf

25 Zurab Bezhanishvili, "Georgia's Political Enigma: Where Does the Political Compass of the Georgian Government Point?" (2024): 8-9, DOI: 10.13140/RG.2.2.21879.12961

26 David B. Carment and Dani Belo, "Non-State Actors and Conflict Management in an Era of Grey Zone Conflict," in *Routledge Handbook of Peace, Security and Development*, ed. Fen Osler Hampson and Alpaslan Özerdem (London: Routledge, 2020), 150

27 For example, democratic backsliding in Georgia happening now. A/N

28 European Parliament, "European Parliament resolution of 2 April 2025 on the implementation of the common foreign and security policy – annual report 2024, P10_TA(2025)0057," European Parliament, April 2, 2025, accessed October 2, 2025, https://www.europarl.europa.eu/doceo/document/TA-10-2025-0057_EN.html

“EURHRTs”,²⁹ Regional StratCom units³⁰, and the “Hybrid Toolbox”³¹—its fragmented response remains insufficient. These are complemented by NATO’s modernization efforts, including the Palantir Maven Smart System,³² Task Force X, commercial satellite partnerships³³, and the 2024 Cognitive Warfare Concept³⁴. Unchecked, such tactics may destabilize even stable EU states, including Germany, Spain, and the UK.

A growing parallel threat is China’s assertive global posture. In alliance with Russia and supported by Iran and North Korea, China seeks to reshape maritime, cyber, and space domains under its control. It has revived its “Three Warfares” and “Unrestricted Warfare” frameworks,³⁵ further institutionalized through the 2024 creation of three new military branches: the “Information Support Force”, “Cyberspace Force”, and “Aerospace Force”.³⁶ These reflect a shift to AI-enabled cognitive warfare, targeting both civilian and military domains.³⁷ The “Tianjin SCO Summit” and China’s 2025 military parade marked a geopolitical turning point. In response, the U.S. is expected to evolve its doctrine—moving from reactive deterrence to proactive, technology-driven hybrid strategies focused on perception, influence, and systemic disruption.³⁸ Traditional tools (sanctions, diplomatic pressure, information fog) will be merged with AI-enabled operations and layered digital engagement. Military leadership must prepare for a new operational reality—the potential emergence of the “First Global Digital War” or a global Technological battle of high-tech specialists—involving both digital and conventional domains. Hybrid warfare will aim not at total control, but at weakening adversaries, displacing influence, or undermining the stability of contested domains. As technological complexity grows, no actor will fully dominate the gray zones. Conflict will increasingly emerge in forms requiring leadership to operate under the following conditions:

- *Information isolation.*
- *Fragmented communication across digital enclaves.*
- *Command without consistent communication.*
- *Governance under persistent or cyclical global conflict.*

29 Council of the European Union, “Hybrid threats: Council paves the way for deploying Hybrid Rapid Response Teams,” press release, May 21, 2024, accessed October 2, 2025, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/?utm_source

30 European External Action Service, “EEAS Strategic Communication Task Forces,” accessed October 2, 2025, https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en

31 Joint Research Centre, “A New Method to Help Policymakers Defend Democracy against Hybrid Threats,” news announcement, April 20, 2023, accessed October 2, 2025, https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en?utm_source

32 NATO, “NATO Acquires AIEnabled Warfighting System,” press release, accessed October 2, 2025, <https://shape.nato.int/news-releases/nato-acquires-ai-enabled-warfighting-system-#:~:text>

33 Greg Hadley, “Space Force to Base New SATCOM Program on Commercial Designs,” *Air & Space Forces*, July 30, 2025, accessed October 2, 2025, <https://www.airandspaceforces.com/space-force-commercial-designs-satcom-pts-g/>

34 NATO, Allied Command Transformation, “Happening in 2024: Advancements in Cognitive Warfare, MultiDomain Operations, Future Operating Environments, Sweden’s Accession to NATO,” January 8, 2024, accessed October 2, 2025, https://www.act.nato.int/article/happening-in-2024-cognitive-warfare-mdofuture-operating-environments-sweden/?utm_source

35 Yamaguchi Shinji, Yatsuzuka Masaaki, and Momma Rira, “China’s Quest for Control of the Cognitive Domain and Gray Zone Situations”, *NIDS China Security Report 2023* (Tokyo: The National Institute for Defense Studies, 2022), https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A01.pdf

36 https://understandingwar.org/backgrounder/china-taiwan-weekly-update-april-26-2024?utm_source

37 Shannon Vaughn, “AI Dependence and Political Blind Spots Undermine Beijing’s War Strategy,” *Foreign Policy Research Institute*, March 2025, <https://www.fpri.org/article/2025/03/ai-dependence-and-political-blind-spots-undermine-beijings-war-strategy/>

38 Zurab Bezhaniashvili “Trump Cards” of Democracy: Winning The Game Against Autocracy,” *Ukraine Analytica Issue 1* (36), 2025 <https://ukraine-analytica.org/wp-content/uploads/Bezhaniashvil.pdf>

Toward Resilient Leadership in an Age of Distrust

Civil and military Informational Society Leaders (ISLs) now operate in a saturated, fragmented information space where shared epistemic ground is absent. Their challenge is not only to command—but to remain “believable” in an environment shaped by rapid decision cycles, sensory overload, and real-time disinformation.³⁹ Malign actors no longer need to dismantle communication systems; they now “weaponize ambiguity”⁴⁰—using AI-enhanced media manipulation, institutional impersonation, and false-flag messaging to erode trust in leadership, alliances, and democratic institutions. In this battlespace, ISLs must manage “epistemic uncertainty”, resist influence operations, and provide moral and informational clarity.⁴¹ Military doctrine must evolve—from physical confrontation to cognitive resilience, from operational art to narrative coherence. Ethical leadership, strategic communication, and digital literacy are now operational imperatives.⁴² Hybrid warfare blurs moral and legal boundaries, with actions falling below formal thresholds of war but carrying serious ethical consequences.⁴³ Leaders now face dilemmas such as AI-generated deception, influence campaigns targeting civilians, and the line between communication and propaganda. Here, ethical leadership, as Peter Northouse describes, becomes vital. Such leadership shapes organizational culture through honesty, justice, and service, sustaining legitimacy even when adversaries show no restraint.⁴⁴ Moral clarity cannot be imposed. It must be cultivated through education, dialogue, and example, especially within increasingly diverse and digitally aware ranks that demand authenticity from leadership. Traditional military doctrine depends on clarity of command, unity of effort, and timely decisions—principles reliant on stable information and hierarchies. Hybrid threats disrupt this foundation by flooding the environment with fabricated reports, conflicting narratives, and deepfakes, compromising situational awareness.⁴⁵ Leaders now operate under epistemic insecurity,⁴⁶ where even battlefield data may mislead. In this context, decision-making tempo becomes a vulnerability: both cautious delays and premature actions based on false inputs can prove damaging.⁴⁷ For example, during the 2014 Crimea annexation, Russian forces operated without insignia and under a media smokescreen, creating confusion and delaying responses from Ukraine and NATO. Today, operational coherence depends not only on intelligence but on trust—in the information ecosystem, subordinate judgment, and institutional integrity.⁴⁸ A relevant parallel is the early COVID-19 response, where governments faced similar uncertainty and disinformation. Yet, many maintained public trust, showing that institutions can, under certain conditions, resist epistemic insecurity. Similarly, during the 2016 U.S. presidential election, foreign

39 Verrall, Neil, and David Mason. 2018. “The Taming of the Shrewd: How Can the Military Tackle Sophistry, ‘Fake’ News and Post-Truth in the Digital Age?” *The RUSI Journal* 163 (1): 20–21. <https://www.rusi.org/explore-our-research/publications/rusi-journal/taming-shrewd-how-can-military-tackle-sophistry-fake-news-and-post-truth-digital-age>

40 Mark Galeotti, “*The Weaponisation of Everything: A Field Guide to the New Way of War*” (New Haven, CT: Yale University Press, 2022), 5

41 Steven Metz, “The Future of Strategic Leadership,” *Parameters* 50, no. 2 (Summer 2020): 63–64, <https://doi.org/10.55540/0031-1723.1020>

42 Adam-Turner, Nancy and Dana D. Burnett. “Leadership Perspectives of Digital Learning and Digital Literacy Adoption at Rural Community Colleges,” *The Community College Enterprise* 24 (2018): 21–22.

43 Afonso Seixas-Nunes, “The Legality and Accountability of Autonomous Weapon Systems: A Humanitarian Law Perspective” (Cambridge and New York: Cambridge University Press, 2022), 65–67

44 Peter G. Northouse, “*Leadership: Theory and Practice*”, 9th ed. (Thousand Oaks, CA: Sage Publications, 2021) 74

45 Dillon Tryhorn, Richard Dill, Douglas D. Hodson, Michael R. Grimaia and Christopher W. Myers. “Modeling fog of war effects in AFSIM,” *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 20 (2021): 135 - 136.

46 Emily Sullivan and Mark Alfano, “*Vectors of Epistemic Insecurity*,” in *Vice Epistemology*, ed. Ian James Kidd, Quassim Cassam, and Heather Battaly (New York: Routledge, 2020), 5

47 Yanling Chang, Matthew F. Kebelis, Ran Li, Eleftherios Iakovou, and Chelsea C. White III, “Misinformation and Disinformation in Modern Warfare,” *Operations Research* 70, no. 3 (2022): 1587 <https://doi.org/10.1287/opre.2021.2253>

48 OECD, “Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust”, *OECD Public Governance Reviews* (Paris: OECD Publishing, 2017), <https://doi.org/10.1787/9789264268920-en>

disinformation campaigns targeted democratic trust and security institutions, illustrating how hybrid strategies can have enduring effects even without kinetic action.

Narrative warfare now overlaps with operational deception, as AI is used to spread disinformation and manipulate military sensors. Adversaries deploy fake satellites, phantom vessels, and radar decoys to mislead automated targeting and overwhelm ISR systems. Deepfakes are no longer limited to human faces—they now include fabricated SIGINT,⁴⁹ spoofed AIS ship locations,⁵⁰ or false satellite telemetry intended to simulate fleet movement⁵¹ or missile deployments. This level of technical deception necessitates that ISLs develop not only strategic communication skills, but also cross-domain literacy in identifying and interrogating compromised sensory and algorithmic data. Absent such capabilities, decisions risk being shaped less by intelligence deficits than by misplaced confidence in corrupted inputs. Resilient command demands systems that foster internal trust, sustain communicative clarity, and institutionalize informed skepticism. Without this adaptive competence, the information society risks not merely isolation, but strategic incapacitation. To prevent this, leadership must evolve operationally, ethically, and cognitively—integrating new literacies that match the complexity of hybrid and algorithmic threats.⁵²

Rapid technological change and emerging threats have created a severe shortage of qualified specialists and capable leaders.⁵³ This overload leads to burnout, critical errors, and the declining effectiveness of institutions—from the UN to national governments. In high-stress, contested information environments, leadership cohesion is further eroded. Younger personnel, though digitally immersed, are often more vulnerable to manipulation and disinformation.⁵⁴ Constant exposure to competing narratives creates confusion, division, and information fatigue. To remain effective, leadership must evolve. James Burns' transformational leadership model is essential: leaders must inspire through vision, trust, and shared purpose—not rely solely on authority. Leadership today must act as a trust network built on transparent, values-based, and interactive communication.⁵⁵ Digital fluency—including awareness of cognitive overload and influence tactics—is now essential. To prevent burnout, institutions must build systems that support ongoing growth, mutual development, and adaptive capacity. Only such environments can sustain resilient leadership in an increasingly complex world.

49 Maj. Gen. Rick Appelhans and Maj. Gen. Ryan Janovic, "Harnessing SIGINT and EW for Tactical Dominance: A Guide for Combat Arms Leaders", June 13, 2025. https://www.army.mil/article/286341/harnessing_sigint_and_ew_for_tactical_dominance_a_guide_for_combat_arms_leaders#:~:text=leaders#:~:text=

50 Thomas Mellor, "Jamming and Spoofing of GNSS and AIS Signals", UK Hydrographic Office, August 11, 2025, <https://www.admiralty.co.uk/news/jamming-and-spoofing#:~:text=>

51 Björn Bergman, "Systematic Data Analysis Reveals False Vessel Tracks," SkyTruth, July 29, 2021, <https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/>

52 János Csombók "Framing Leadership Challenges in the Digital Age: The Role of Senior Leaders." *Hadtudomány* 33, no. 2 (2023): 102. <https://doi.org/10.17047/HADTUD.2023.33.2.95>

53 Nate Paynter et al., "Navigating the Tech Talent Shortage," *Deloitte Insights*, June 11, 2024, <https://www.deloitte.com/us/en/insights/topics/talent/overcoming-the-tech-talent-shortage-amid-transformation.html>

54 Maxime Kops, Catherine Schittenhelm, and Sebastian Wachs, "Young People and False Information: A Scoping Review of Responses, Influential Factors, Consequences, and Prevention Programs," *Computers in Human Behavior* (August 2025), 169 <https://doi.org/10.1016/j.chb.2025.108650>

55 Gaston, David W. "The Transformational Leader: Managing Organizational Trauma Through Seasons of Change." In *Role of Leadership in Facilitating Healing and Renewal in Times of Organizational Trauma and Change*, edited by Lynda Byrd-Poller, Jennifer L. Farmer, and Valerie Ford, Hershey, PA: IGI Global Scientific Publishing, 2021, 46-47.

Conclusion

In the era of total distrust and rapid digital transformation, leadership must adapt to a fundamentally altered strategic landscape. Strategic communication is no longer peripheral—it is operationally essential for legitimacy and cohesion. Civilian and military leaders alike must prepare for full-spectrum digital warfare, including hybrid and WMD-based threats. As societies fragment into digitally aware and unaware cohorts, leadership must employ perception-sensitive, tailored communication to maintain resilience. Modern leaders must operate seamlessly across kinetic and cognitive domains, institutionalizing “cognitive hygiene” practices to safeguard mental clarity. Understanding how various groups process information is critical to countering disinformation and sustaining narrative coherence. Future conflicts will engage entire populations, not just elites, necessitating culturally embedded, participatory training in digital discipline. Trust networks—interpersonal and institutional—form the backbone of societal defense against manipulation. Above all, information integrity must be elevated to a strategic function. This evolving reality demands integrated, universal, and ethically grounded civil-military leadership capable of commanding trust.

In contemporary strategic environments, the erosion of public trust is no longer a peripheral concern—it has become a central axis of conflict. The destabilization of shared meaning occurs not solely through falsehoods, but through the selective amplification of truths stripped of context. Much like overusing a single pigment in the printing process distorts the final image, adversarial actors exploit the epistemic openness of liberal societies by disproportionately emphasizing emotionally charged narratives—grievance, fear, or historical trauma—until the broader informational spectrum collapses into affective saturation. This does not require fabricating disinformation; rather, it turns the informational richness of open societies against themselves. In such a terrain, total distrust is not an unintended consequence of the digital age, but a deliberately cultivated condition—an outcome of epistemic imbalance engineered to paralyze deliberation, fracture social cohesion, and delegitimize institutions. The strategic challenge lies in the fact that even truth, when decontextualized and weaponized, becomes a vector of instability. Institutional responses—often reactive or overly technocratic—risk reinforcing the problem by appearing disconnected from public sentiment or incapable of narrative empathy. To navigate this landscape, leadership must be redefined as an epistemological function as much as a strategic one. The modern leader—civilian or military—can no longer rely solely on hierarchical authority or traditional operational competencies. Instead, they must serve as custodians of narrative integrity, capable of discerning not only what is being said, but how, why, and to what emotional effect. This demands proficiency in narrative literacy, discursive ethics, and cognitive hygiene, as well as a deep understanding of how diverse populations process and respond to information under stress. Moreover, the emerging threat landscape demands preparedness across both kinetic and cognitive domains. Civilian and military leaders alike must prepare for full-spectrum digital warfare, encompassing hybrid operations, disinformation campaigns, and weapons of mass destruction. These threats are no longer confined to the battlefield—they target societal trust, institutional legitimacy, and the psychological resilience of populations. Indeed, future conflicts will engage entire societies, not just militaries or political elites. This reality requires the construction of new forms of social

defense—adaptive, participatory systems of collective resilience capable of responding to both local and global threats, including those of mass destruction. These systems must be culturally embedded and reflexively governed, designed not only to repel external adversaries but also to prevent the internal fragmentation of social trust. Within this broader strategic architecture, information integrity must be institutionalized as a core national function, on par with intelligence, cyber operations, and logistics. In an age where perception is both a target and a terrain of warfare, trust becomes not a byproduct of stability, but its precondition. Building and sustaining this trust requires deliberate cultivation of interpersonal, institutional, and transnational networks grounded in ethical leadership and transparent communication. In conclusion, the future will not be secured by technology alone, nor by force of arms. It will depend on the emergence of integrated, ethically grounded, and epistemologically agile leadership—leaders capable of commanding trust in fragmented societies, moderating polarized narratives without suppressing dissent, and guiding populations through the fog of information war. In this new age of strategic complexity, leadership is no longer just about command—it is about coherence, cognition, and the continuous recalibration of meaning in a contested world.



From Bayonets to Bits and Bytes: Leadership in the Information Environment

Commandant Killian Doyle

Abstract

The modern battlespace is no longer confined to physical terrain; it is shaped by cyber threats, hybrid tactics, influence operations, and cognitive warfare. Leadership within this environment must evolve accordingly. This article examines how contemporary commanders must adapt, building cognitive resilience, navigating disinformation, and leading across blurred domains of peace and conflict. Drawing on international examples and recent case studies, it argues that traditional leadership models must integrate digital literacy and critical thinking, while institutional reforms are needed to develop specialist career paths for emerging domains such as cyber and information warfare.

"The most important six inches on the battlefield is between your ears."

— General James N. Mattis, USMC (Ret.)

Introduction: Command Beyond the Kinetic

Military leadership today can no longer be confined to the physical domain or traditional kinetic operations. Contemporary military activity now takes place where physical, cyber, and cognitive domains intersect and influence one another. Today, threats are coded as much as they are constructed, often delivered through malware, misinformation, and manipulation rather than conventional munitions. The emergence of Artificial Intelligence (AI), autonomous cyber capabilities, and algorithmically driven influence campaigns has altered not just the tools of conflict, but also its tempo and terrain.

Hybrid warfare blurs the lines between war and peace, truth and falsehood.¹ Enabled by digital tools and social media, a lone actor can now shape perception, disrupt systems, and tilt regional balance. NATO's evolving posture reflects this shift.² From the 2007 cyberattacks on Estonia to the recognition of cyberspace as a domain of operations in 2016, the alliance has steadily adapted. NATO's CCDCOE³ in Tallinn and Hybrid COE in Helsinki show commitment to addressing these threats. Joint exercises now test not only technical defences, but also the strategic coordination of allied forces under pressure.

These developments have fundamentally reshaped the leadership landscape. Military leaders are now required to operate across multiple domains while navigating an information environment saturated with deception, distraction, and deliberate ambiguity. As we will see, such environments exacerbate cognitive biases and stress-based decision-making. Understanding the psychological dimension of conflict is no longer optional; it is essential.

1 Andrew Mumford and Pascal Carlucci. "Hybrid Warfare: The Continuation of Ambiguity by Other Means," *European Journal of International Security* 7, no. 1 (2022): 24–42.

2 Daniele Genini, "Countering Hybrid Threats: How NATO Must Adapt (Again)," *Global Security: Health, Science and Policy* (2025)

3 Cooperative Cyber Defence Centre of Excellence

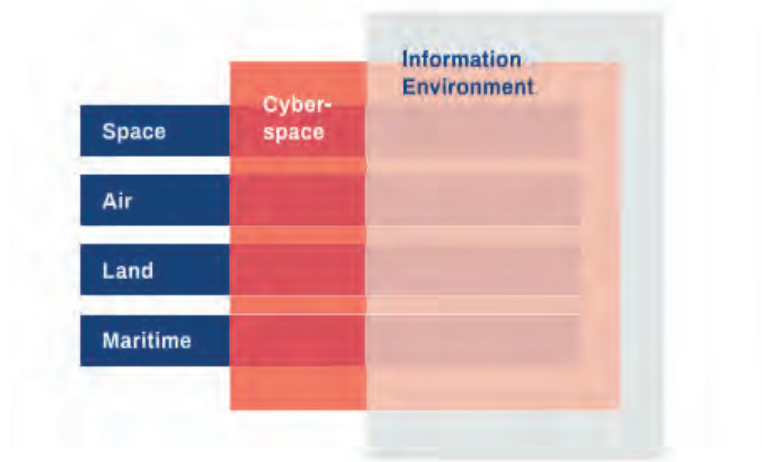


Figure 1: 21st Century Battlespace Domains and the Information Environment ⁴

In the Irish Defence Forces (DF), leadership development has traditionally followed a generalist model, producing adaptable operational leaders through rotational appointments. While this approach has strengths, it leaves emerging domains such as cyber and information operations without the depth of expertise they increasingly require. This status quo provides the baseline against which we explore what leadership means in this transformed context. This paper examines how the convergence of cyber threats, hybrid tactics, and cognitive operations demands new thinking, new skills, and new models of command. Drawing on contemporary doctrine, behavioural science, and real-world case studies, this paper argues for a broader conception of leadership—one that complements traditional command with critical thinking, digital literacy, and cognitive resilience, and encompasses mastery of information, influence, and the human dimension of conflict.

Cognitive Leadership in Contemporary Conflict

Traditionally, military leadership has always involved navigating uncertainty, deception and psychological pressure, yet today’s leaders face these challenges at an amplified scale as digital technologies increase the intensity with which they challenge decision making and cohesion.⁵ Increasingly, it is contested in the cognitive space, where perceptions, beliefs, and behaviours are shaped by the information environment. The integration of cyber, information, and psychological operations has established the human mind as a central domain of engagement. In conflicts such as the Russo-Ukraine war, influence operations have become central tools to degrade public trust, manipulate perception, and fracture

4 Frank Hickey, Battista Magurno, Sergio Pastor, Nuno Rodrigues, and Damjan Štruel, eds., *Cyber Commanders' Handbook 2* (Tallinn: NATO CCDCOE Publications, 2025): 79.

5 Arijana Marjanović and Dražen Smiljanić, "Cognitive Warfare – the Human Mind as the New Battlefield," *Proceedings of the Defence and Security Conference* (April 2025), 1, no.1, 84-114

political cohesion.⁶ As noted in an article published by the U.S. Army War College, “the threat of influence no longer exists only during deployment but also in garrison because of ‘the collapsed nature of communication . . . and . . . porous boundaries between war and everyday life’”.⁷

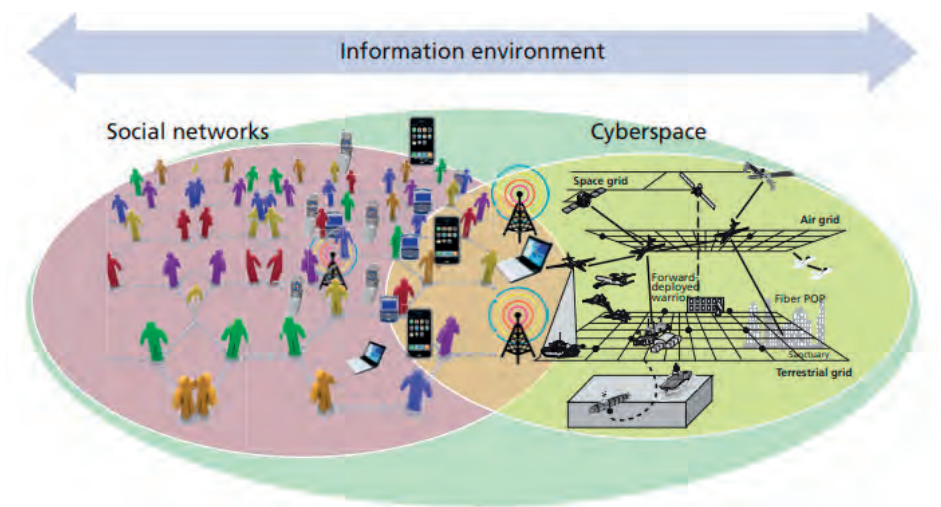


Figure 2: Cyberspace and Social Networks in the Information Environment⁸

This form of warfare targets not just national populations, but the militaries themselves. As part of society, soldiers and commanders are exposed to the same algorithms, emotional triggers, and biases that adversaries exploit. Adversaries often see military personnel as attractive targets, with evidence showing widespread and coordinated disinformation campaigns aimed at service members.⁹ These influence efforts extend well beyond disinformation campaigns. In 2019, NATO’s Strategic Communications Centre of Excellence demonstrated how a modest investment in ‘sock puppet’¹⁰ social media accounts could gather sensitive operational information, influence personnel behaviour, and even prompt soldiers to abandon their posts; all achieved using just \$60 of targeted ads.¹¹ A repeated warning came from the experiment’s director: “Every person has a button...

6 Peter B.M.J. Pijpers, *Exploiting Cyberspace: International Legal Challenges and the New Tropes, Techniques and Tactics in the Russo-Ukraine War*, Hybrid CoE Paper 15 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2022): 8–9.

7 Meghan Fitzpatrick, Ritu Gill & Jennifer F. Giles, “Information Warfare: Lessons in Inoculation to Disinformation,” *Parameters* 52, no. 1 (2022): 109, doi:10.5554/0031-1723.3132.

8 Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, and Bruce J. Held, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, (Santa Monica, CA: RAND Corporation, (January 2013), <https://www.rand.org/pubs/monographs/MG1113.html>

9 Ibid

10 A **sock puppet** is a false online identity used to deceive, influence, or gather information; while commonly associated with disinformation, such accounts are also used by open-source investigators for covert observation and research.

11 Sebastian Bay, Giorgio Bertolin, Nora Biteniece, Edward H. Christie, Anton Dek, Rolf E. Fredheim, John D. Gallacher, Kateryna Kononova, Tetiana Marchenko, *Responding to Cognitive Security Challenges* (Riga: NATO Strategic Communications Centre of Excellence, 2019): 8-12

what's openly available online is sufficient to know what that is".¹² These vulnerabilities are now being amplified by AI, which can rapidly synthesise personal data to generate highly tailored influence content; automating what was once manual manipulation and doing so at unprecedented scale.¹³

AI systems now deliver tailored disinformation, while autonomous tools conduct reconnaissance, scanning, and adaptive malware deployment. Such tools alter both the tempo and complexity of the digital battlespace, compressing decision cycles and demanding leadership that is comfortable with rapid, informed risk assessment. In a real-world, kinetic environment, such vulnerabilities have also been exploited in the ongoing war in Ukraine, where Russian actors have repeatedly targeted individual soldiers through personal devices and emotional manipulation tactics to degrade morale, sow confusion and compromise operational security.¹⁴ The takeaway for commanders is clear: a single post can expose an entire unit. The digital behaviour of individual soldiers can undermine collective security; when personal content reveals unit activity, sentiment, or location, adversaries gain insight into morale, readiness, and command posture.

Understanding how and why these efforts succeed begins with an appreciation of human cognition. Daniel Kahneman's seminal work on the dual-system model of thinking is central to this.¹⁵ In high-pressure, high-uncertainty environments, common in both conventional and hybrid warfare, leaders tend to rely on System 1 thinking, which is fast, intuitive, and emotionally driven. While useful in some tactical situations, it is also susceptible to bias. System 2 is slower and more deliberate, but harder to access under stress. Kahneman's concept of "What You See Is All There Is" (WYSIATI) explains how humans instinctively accept the first, often emotionally charged, version of an event, particularly when it is presented visually or socially validated.¹⁶

Adversaries in the hybrid domain understand this deeply. Disinformation campaigns are designed to exploit confirmation bias, availability bias, and emotional reasoning, undermining leaders' ability to apply deliberate, analytical judgement. "Individuals accept information that is congruent with their perspective as opposed to taking the time to process information that is contradictory".¹⁷ This is why disinformation often plays on race, immigration, religion, and other divisive issues: not because they are necessarily relevant to military objectives, but because they bypass rational scrutiny and corrode internal cohesion. Influence operations frequently employ polarising content designed to divide groups and erode cohesion.

12 Lily Hay Newman, "How NATO's Fake Social Media Accounts Tricked Soldiers," *Wired*, March 4, 2019, <https://www.wired.com/story/nato-stratcom-cattified-soldiers-social-media/>.

13 Perry Carpenter, *FAIK: A Practical Guide to Living in a World of Deepfakes and Information Disorder* (Montgomery, AL: Wiley, 2024): 133–156.

14 Dan Black, "Russia's Cyber Campaign Shifts to Ukraine's Frontlines," *Royal United Services Institute*, July 22, 2024, <https://www.rusi.org/explore-our-research/publications/commentary/russias-cyber-campaign-shifts-ukraines-frontlines>.

15 Daniel Kahneman, "A Perspective on Judgment and Choice: Mapping Bounded Rationality," *American Psychologist* 58, no. 9 (2003): 699–701.

16 Daniel Kahneman, *Thinking, Fast and Slow* (London: Penguin, 2011), 20–21, 45–46, 85–88.

17 Fitzpatrick et al., "Information Warfare: 108

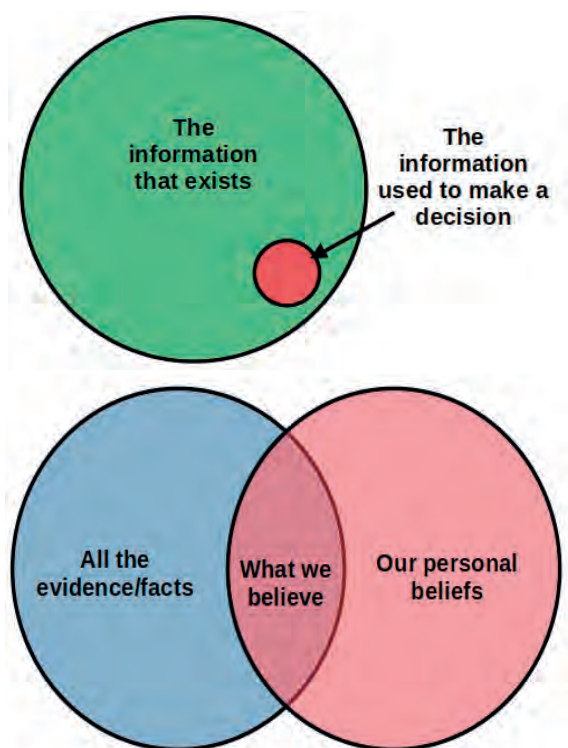


Figure 3: Availability Bias and Confirmation Bias (author's own)

These insights reinforce a critical shift in leadership towards fostering resilience and information awareness within teams. Tactical acumen remains essential, but it must be matched by cognitive resilience, psychological awareness, and media literacy. Commanders must navigate ambiguity, interpret conflicting information, and lead in contested domains where even the nature of conflict is unclear. Hybrid threats exploit this ambiguity, operating across legal, psychological, and digital domains. As one UK Defence Secretary put it, they exist “in that limbo land between peace and war.”¹⁸

This convergence has somewhat disrupted the utility of traditional tools. The Military Decision-Making Process (MDMP) remains useful for structured planning and ensuring clarity across command levels. It provides *detailed* thinking, but not necessarily *critical* thinking. While it promotes procedural rigour and convergence, it does not inherently challenge assumptions.¹⁹ Without deliberate efforts to encourage dissent, it can unintentionally suppress innovation. Over-reliance on structure also risks enabling groupthink, a phenomenon Janis linked to loyalty overriding critique, especially under

¹⁸ Dominic Nicholls, “SAS Ordered to Start Disrupting Russian Meddling around the World,” *Telegraph*, March 20, 2021, <https://news.yahoo.com/sas-takes-fight-meddling-russians-194726397.html>.

¹⁹ U.S. Army, *FM 6-0: Commander and Staff Organization and Operations* (Washington, DC: HQDA, May 2014), 7-2; U.S. Army, *FM 5-0: Army Planning and Orders Production* (Washington, DC: HQDA, 2022): ch. 3.

stress.²⁰ Symptoms like collective rationalisation and illusion of unanimity reflect cognitive traps well known in behavioural science. Kahneman's concept of anchoring shows how early ideas distort subsequent reasoning.²¹ Grimes adds further examples, such as correlation errors, biases and logical fallacies.²² Although the Operational Planning Process (OPP) incorporates mechanisms intended to surface assumptions and encourage reflection, most leaders do not encounter this process until relatively senior in their career. As a result, exposure to critical reflection and assumption-testing may come too late to shape the every-day military decision making culture. Such reasoning flaws are commonly taught in intelligence analyst training,²³ but are not always embedded in early leadership development. Though drawn from outside the military sphere, Grimes' discussion of the discredited link between the MMR vaccine and autism underlines how emotional narratives can eclipse evidence.²⁴ Such examples reinforce the earlier point that without reflective practice, decision-making can fall prey to logical fallacies and a lack of critical thinking. That vulnerability is now amplified by algorithms and AI, which rapidly deliver targeted influence.²⁵ This speed and precision reinforce the need for leaders who can detect and counter manipulation in the cognitive domain.

This gap in critical reasoning education leaves decision-makers exposed in environments saturated with manipulated information and emotionally charged narratives. Amid the rise of narrative warfare, these tendencies can be exploited strategically, with adversaries using online influence to reinforce pre-existing beliefs within a force, sow distrust, and induce paralysis. In the age of disinformation, perception itself becomes the battleground, where influence replaces direct coercion as the mechanism of control.²⁶ This framing is reinforced by Fitzpatrick *et al.*, who argue that "Service members and their families must learn and practice media literacy skills so they can protect themselves and counter adversary initiatives."²⁷ Cognitive security is therefore not a peripheral concern; it is a force protection issue.

Leadership, then, must evolve. The commander of today requires not only doctrinal fluency and operational competence, but also the ability to detect cognitive manipulation, foster open information environments, and build team resilience against emotional and ideological subversion. Finland offers an instructive case here. Its cross-sectoral approach to media literacy, teaching students, journalists, and public officials to identify *deepfakes* and fake news,²⁸ illustrates a model of resilience-building that should inform leadership and policy recommendations.

In summary, military leaders cannot afford to treat disinformation and psychological manipulation as externalities. These tactics are aimed not just at populations or strategic objectives, but at undermining internal trust, degrading decision-making, and fracturing cohesion. Armed with insights from behavioural science, and supported by reforms in

20 Irving L. Janis, *Victims of Groupthink: A Psychological Study of Foreign-Policy Decisions and Fiascos* (Boston: Houghton Mifflin, 1972).

21 Kahneman, "Perspective on Judgement and Choice".

22 David Robert Grimes, *The Irrational Ape: Why Flawed Logic Puts Us All at Risk and How Critical Thinking Can Save the World* (London: Simon & Schuster, 2019): 104, 150, 215, 229, 338.

23 Richard J. Heuer Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence): 127-146.

24 Ibid.

25 Carpenter, *FAIK*: 133-156.

26 Ibid: 4-17, 164.

27 Fitzpatrick *et al.*, "Information Warfare: 115.

28 William Marcellino *et al.*, *Human Machine Detection of Online Based Malign Information* (Santa Monica, CA: RAND Corporation, 2020): 11-13.

training and doctrine, military leadership must adapt: not by abandoning tradition, but by enhancing it with the cognitive tools demanded by modern conflict. The cognitive dimension is only one element of this evolving operational environment. Leaders must also contend with the complexities of hybrid and cyber battlespace command, where technical, legal, and strategic challenges further shape modern conflict.

Command and Leadership in the Hybrid-Cyber Battlespace

While cognitive security represents one of the most pressing leadership challenges of the modern era, it is only one front in a wider contest. Commanders today must also exercise leadership across technical, legal, and operational dimensions, often in real time, under conditions of extreme ambiguity. This is particularly evident in the hybrid and cyber battlespace, where the tempo of engagement outpaces conventional decision cycles and where attribution, legal clarity, and traditional command structures frequently fall short.

The so-called “grey zone” of modern conflict is no longer a theoretical space. In practice, it is populated by non-state actors, information proxies, and strategic behaviours calibrated to avoid breaching traditional thresholds for military response. Leadership in this space demands comfort with complexity. Attribution remains a persistent challenge: as demonstrated in high-profile case studies of Russian cyber operations, state actors routinely leverage proxies, false flags, and asymmetric techniques to sow confusion and delay responses.²⁹ The legal consequences are significant. As articulated in the *Tallinn Manual 2.0*, certain cyber operations may constitute a use of force under international law, however, determining authorship, intent, and proportionality is anything but straightforward.³⁰ For commanders, this legal ambiguity complicates not only operational planning but also the framing of response authorities and rules of engagement in cyberspace. These evolving interpretations highlight the need for leadership attuned to both legal nuance and operational agility.

This ambiguity is further compounded by the presence of actors outside conventional chains of command. During the war in Ukraine, companies such as Microsoft and SpaceX played decisive roles in shaping the battlespace by identifying and countering malware deployed by Advanced Persistent Threat (APT) ³¹ groups and cybercrime organisations, restoring connectivity, and even influencing operational tempo.³² Investigative organisations like Bellingcat³³ have shaped narratives and uncovered war crimes using open-source intelligence, often outpacing state intelligence services.³⁴ ³⁵ These developments redefine the operating environment. Influence, access, and initiative are not confined to uniformed actors, yet their outcomes directly affect military objectives and strategic decisions.

29 Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019).

30 Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017): 331–336.

31 An APT is a well-resourced threat actor, often state or state-aligned, targeting specific entities to gain ongoing access to systems/information.

32 Peter B.M.J. Pijpers, *Exploiting Cyberspace: International Legal Challenges and the New Tropes, Techniques and Tactics in the Russo-Ukraine War*, Hybrid CoE Paper 15 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2022): 8–9.

33 Bellingcat is an independent investigative collective founded in 2014, specialising in the use of open-source intelligence (OSINT) such as satellite imagery, social media, and geolocation to investigate issues including armed conflict, disinformation, and war crimes. See: Bellingcat, “About Bellingcat”, accessed August 25, 2025, <https://www.bellingcat.com/about>

34 Eliot Higgins, *We Are Bellingcat: An Intelligence Agency for the People* (London: Bloomsbury, 2021): 11–14.

35 Alexa O'Brien, “Open Source Intelligence May Be Changing Old School War,” *Wired*, May 24, 2022, <https://www.wired.com/story/ukraine-war-open-source-intelligence-osint>.

Ireland offers a timely case study of how even politically neutral states remain vulnerable to the realities of modern cyber conflict. Its traditional policy of military neutrality, while politically enduring and politically nuanced, is not a shield in cyberspace where state-aligned cyber threat actors can cause strategic harm regardless of declared intent or jurisdiction. The 2021 ransomware attack on Ireland's HSE had strategic impact; paralyzing hospitals, exposing data, and demanding a national and international response.³⁶ These complexities highlight the ongoing uncertainty surrounding attribution, whether the assault was state-orchestrated, criminal, or any combination thereof, and serve as a salient reminder that Ireland's cyber exposure is real, growing, and far beyond the reach of passive neutrality.³⁷ Legal commentary increasingly recognises that neutrality in cyberspace offers no blanket exemption from the responsibilities of international law. States are expected to exercise due diligence in protecting their networks and preventing their infrastructure from being exploited to harm others.³⁸ Inaction in the face of known threats may itself be seen as a failure of obligation.³⁹ In this context, a posture of passive defence is neither credible nor sustainable.

Recognising this evolving landscape, the 2022 Commission on the DF recommended establishing a Joint Cyber Defence Command (JCDC) and strengthening joint structures across the organisation, including enhanced cyber and intelligence capabilities.⁴⁰ Yet the success of these initiatives will depend not only on new organisational charts, but on evolving leadership models that value deep domain expertise. As outlined earlier, traditional DF generalist career progression is designed to produce broad operational leaders through rotational appointments. While this model remains effective in certain contexts, it is increasingly misaligned with domains that demand technical proficiency, long-term continuity, and joint operational fluency.⁴¹ As the Commission itself reported, widespread frustration persists regarding career planning and personnel management, particularly the lack of HR structures to retain and develop specialist skills.⁴² Generalist leadership models excel at producing flexible operational leaders, but are poorly suited to domains where mastery of fast-evolving technology, legal nuance, and cross-sector coordination is essential. Rotational models risk eroding hard-won expertise just as it becomes most valuable, while joint and cyber operations demand deep domain fluency that cannot be built through short-term appointments. Without deliberate cultivation of specialist career paths—and a leadership culture acknowledging that sometimes, expertise matters more than a well-rounded posting history—emerging commands risk a deficit of credible, expert leadership, a concern raised in recent U.S. Naval Institute commentary.⁴³

36 PricewaterhouseCoopers, *Conti Cyber Attack on the HSE: Independent Post Incident Review*, commissioned by the HSE Board (Dublin: HSE, December 3, 2021), <https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>.

37 "Ireland's neutrality does not stop it from being eyed as a cyber target," *Irish Examiner*, September 7, 2024.

38 Jan Martin Lemnitzer, "Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace," *European Journal of International Law* 33, no. 3 (2022): 802, 815.

39 Schmitt, *Tallinn Manual* 2.0: 26

40 *Report of the Commission on the Defence Forces* (Dublin: Department of Defence, February 2022), sections 7.6: 24–26.

41 Erica Loneragan and Mark Montgomery, *United States Cyber Force: A Defense Imperative* (Washington, DC: Foundation for Defense of Democracies, March 2024).

42 *Ibid.*, sections 9.11–9.12.

43 Eric Seligman, "Changing the Cyber Warfare Leadership Paradigm," *Proceedings*, U.S. Naval Institute, June 2023.

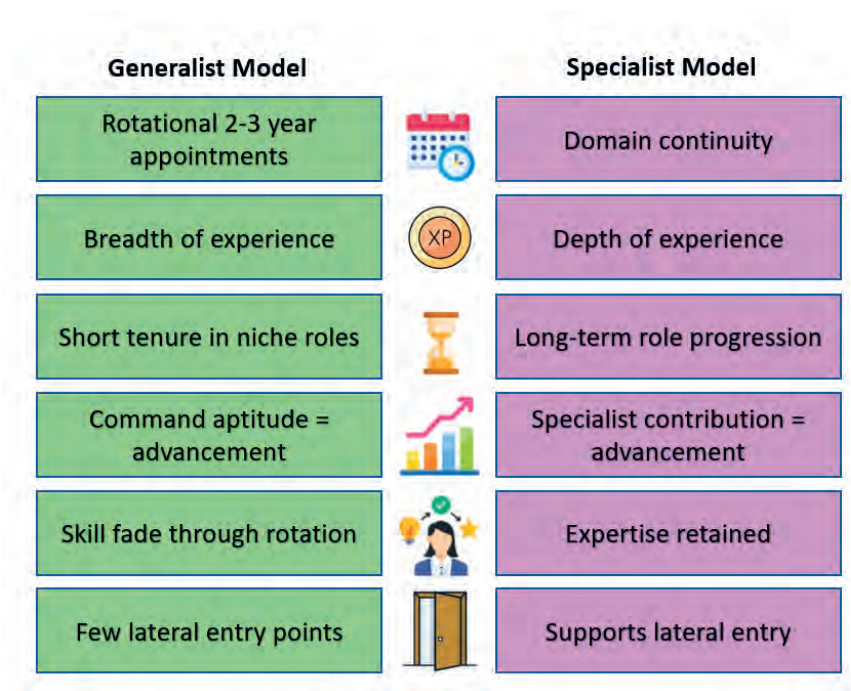


Figure 4: Generalist vs Specialist Career Models (author’s own)

Institutional Shifts for Modern Military Leadership

Meeting these leadership challenges requires not only operational change, but cultural evolution across the DF. As this paper has demonstrated, modern commanders must contend with adversaries ranging from APT groups to autonomous systems, in an environment where perception, cognition, infrastructure, and legal ambiguity all form a contested battlespace.

Actionable Recommendations

To address the demands of today’s multi-domain conflicts, military leadership should prioritise the following actions:

- 1. **Embed cognitive security as a leadership and force protection priority.** Training should integrate media literacy, psychological resilience, and cognitive bias awareness from junior levels onward, treating disinformation and psychological manipulation as deliberate threats to cohesion, decision-making, and operational security. Embedding cognitive security prepares leaders to slow down, question assumptions, and protect both their people and missions from manipulation.

2. **Adapt planning frameworks to counter cognitive bias and groupthink.** Existing tools like MDMP should be complemented by practices that foster critical thinking, challenge assumptions, and avoid convergence, especially in ambiguous, hybrid, or information-driven operations. Leaders should institutionalise practices such as red-teaming, devil's advocate and structured dissent as measures to prevent the kinds of logical fallacies and distorted reasoning that undermine organisational cohesion.
3. **Develop and reward domain-specific leadership pathways.** Cyber, intelligence, and information operations leadership should follow specialist tracks that foster continuity and depth, avoiding over-reliance on rotational models. As identified in other militaries, specialist leaders should have dedicated career streams. Without continuity, the DF risks losing critical expertise at precisely the moment when these domains are most decisive.
4. **Contribute to whole-of-society resilience and prepare for grey zone conflict.** Military leadership should support national resilience efforts through cross-sector collaboration and ensure leadership education, planning, and exercises reflect Ireland's vulnerability to sub-threshold hybrid and cyber threats. As has been seen, neutrality does not confer immunity; Ireland's status as a technological hub and undersea cable infrastructure makes it an attractive target. Military leadership must therefore emphasise engagement with civilian partners, drawing lessons from how various actors have influenced conflicts and shaped narratives from beyond traditional state lines.
5. **Design exercises to reflect modern conflict complexity.** Exercises should expose leaders to legal, cognitive, and narrative dilemmas, fostering comfort operating in ambiguity. International exercises now show how contested legal and informational environments are central to operations. Domestic exercise scenario design should reflect this to deliberately integrate ambiguity, misinformation and competing narratives. Such exercises prepare leaders not just for battlefield complexity, but for the array of challenges of the grey zone.

Conclusion

Leadership in the modern battlespace demands more than operational competence; it requires a new mind-set. As conflict now spans physical, digital, and psychological domains, commanders must be as comfortable navigating uncertainty and complexity as they are leading kinetic operations. From AI-enabled disinformation to hybrid legal challenges, today's leaders face pressures that test not only plans, but perception itself.

This paper has argued that effective military leadership must now combine cognitive insight, digital literacy, and adaptive judgement. These are not abstract ideals, but essential capabilities for sustaining cohesion, clarity, and command in an environment saturated with influence and deception.

Though tactics evolve, leadership remains decisive. With reform, education and understanding of information as power, leaders can meet modern challenges with clarity and effectiveness.



Fog, Friction, Fragmentation: Military Decision-Making in an Age of Mosaic Warfare

Commandant Simon Keenan

“We cannot solve our problems with the same thinking we used when we created them” - Albert Einstein

Introduction

Against the backdrop of renewed strategic competition between major powers, technologies such as autonomous systems and artificial intelligence (AI) are changing the character of war, influencing how military leaders strive to impose order and predictability on the contemporary operating environment.¹ Modern warfighting paradigms that emphasise speed and ubiquity of information represent a shift toward distributed, adaptable and technologically-enabled force structures – ‘mosaic warfare’ is one such concept. Like the tiles in a mosaic, components or systems having certain functional characteristics could be combined to generate emergent effects across multiple domains in real time.² Emphasising autonomy and AI-enabled decision-making, this approach reframes warfare as a complex adaptive system in which tactical encounters can be as globalised as the internet. In such a fragmented and rapidly shifting environment, the operating environment is no longer static or fully knowable; instead, it is emergent and non-linear. When compounded by the exponentially accelerating pace of technological change, new warfare paradigms such as mosaic warfare risk exposing the limitations of traditional decision-making frameworks used by operational and strategic planners.

Established frameworks consist of ‘iterative logical planning methodologies’ used by commanders and staff to overcome the uncertain and unpredictable challenges that complicate military operations – often referred to in Clausewitzian terms as ‘fog’ and ‘friction’.³ This paper explores the implications of mosaic warfare for contemporary military decision-making. Drawing on the conceptual lens of complexity theory, it argues that traditional decision-making frameworks – based on linear cause-effect reasoning – are increasingly redundant in volatile, uncertain, complex and ambiguous (VUCA) operating environments. In contrast, effective command in the age of mosaic warfare demands a prioritisation of sense-making and adaptability. Clausewitz’s ‘fog’ and ‘friction’ cannot be fully eliminated by new technologies or concepts; rather, they are intensified by the fragmentation of the engagement space and the velocity of AI-enabled decision loops. By examining military epistemology, institutional logic, and emerging operational design concepts, this paper calls for a reframing of decision-making beyond process conformity and linear reasoning toward one rooted in emergence and agility.

Understanding the Pieces of the Puzzle

The multi-domain operating (MDO) environment encompasses diverse actors and interconnected variables, expanding the traditional battlespace beyond the physical realm and into the information space enabled through interconnected networks such as the internet. The military elements that engage in tactical encounters today are connected

1 James Johnson, ‘The AI Commander Problem: Ethical, Political, and Psychological Dilemmas of Human-Machine Interactions in AI-Enabled Warfare’, *Journal of Military Ethics* 21, nos. 3–4 (2022): 252, <https://doi.org/10.1080/15027570.2023.2175887>.

2 Benjamin Jensen and John Paschkewitz, ‘Mosaic Warfare: Small and Scalable Are Beautiful’, *War on the Rocks*, 23 December 2019, <http://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/>.

3 Herwin Meerveld et al., ‘The Irresponsibility of Not Using AI in the Military,’ *Ethics and Information Technology* 25, no.1 (2023): 14, <https://doi.org/10.1007/s10676-023-09683-0>.

via a network of systems to multiple sensors and command nodes bringing renewed significance to the term 'strategic corporal'. In this regard, contemporary military strategists and operational planners must consider a broad range of informational, diplomatic and social factors when developing military response options.

'Mosaic Warfare,' as articulated by DARPA's Strategic Technology Office, is a technology-enabled strategic concept consisting of a wide network of interoperable systems that can instantaneously respond to operational needs, creating strategic outcomes through coordinated, networked actions. The goal of mosaic warfare is "to create a chain of effects—or, more accurately because these effects are not linear, 'effects webs'—to deter and defeat adversaries across multiple scales of conflict intensity."⁴ It builds on modern concepts of warfighting, such as algorithmic warfare⁵ and hyperwar⁶ in combining technological innovation with mission command. Militaries adopting this approach seek to offset and outpace adversaries when competing above and below the threshold of war.

The use of AI⁷ to enable modern concepts of warfighting has the potential to overcome the inherent shortcomings of traditional military decision-making such as the over-saturation of data associated with networks of systems. Its use is "symptomatic of a cumulative longer-term effort by militaries to use technology to tame chance and eradicate uncertainty."⁸ Chronicled examples of AI in a defence context include the commercial 'Palantir' system enabling intelligence and logistics continuity by the Ukrainian Armed Forces and the US military's proprietary 'Project Maven' that employs algorithms to detect, classify and present targets to human decision makers before transmitting decisions to a network of automated and human-controlled weapon systems. Closer to home, AI was used to detect Russian 'shadow fleet' vessels operating in Ireland's Exclusive Economic Zone (EEZ) through the cross referencing of satellite imagery with anomalies in shipping data.⁹ It is clear that AI has already advanced to a level where it can be used to automate the collection and analysis of data and curate key insights for decision-makers. Developments in the near future are likely to see warfare taking place at a scale and speed beyond the limits of human cognitive capacity. As such, the loop of action-reaction-counteraction which has informed traditional decision-making frameworks heretofore will become increasingly irrelevant.

Military decision-making has traditionally relied on a linear, reductionist understanding of war. Our system of professional military education (PME) promotes and enforces efforts to tame chance and eradicate uncertainty by "reducing the conduct of war to a set of rules and a system of procedures – and therefore make orderly and rational what is essentially chaotic and instinctive."¹⁰ Contemporary decision-making models such as the Military Decision Making Process (MDMP) or NATO's Operational Planning Process (OPP) evolved from analytical decision frameworks adopted by the US military in the middle

4 DARPA, "Strategic Technology Office Outlines Vision for Mosaic Warfare," 04 August 2017, <https://www.darpa.mil/news-events/2017-08-04>.

5 Peter Layton, *Algorithmic Warfare: Applying Artificial Intelligence to Warfighting* (Canberra: Australian Air Power Development Centre, 2018).

6 John R. Allen and Amir Husain, "On Hyperwar," July 2017, *Proceedings* Vol. 143/7/1, 373.

7 In this article, the term artificial intelligence (AI) refers to computer systems capable of performing tasks normally requiring human intelligence, such as: human-like perception, cognition, analysis, planning, learning, communication or physical action. It does not distinguish between general and limited AI, which is beyond the scope of this paper. (James Johnson [2019], Artificial intelligence & future warfare: implications for international security).

8 James Johnson, "The AI Commander Problem: Ethical, Political, and Psychological Dilemmas of Human-Machine Interactions in AI-Enabled Warfare", *Journal of Military Ethics* 21, nos. 3–4 (2022): 252, <https://doi.org/10.1080/15027570.2023.2175887>.

9 Conor Gallagher, "Dramatic Increase in Number of Russian "Shadow Ships" in Irish-Controlled Waters," *The Irish Times*, accessed 1 August 2025, <https://www.irishtimes.com/ireland/2025/07/21/number-of-russian-shadow-ships-in-irish-controlled-waters-rises-dramatically/>.

10 John Keegan, *The Face of Battle*, (London: Cape, 1976), 20.

of the 20th century, which were themselves rooted in the military innovations of the 19th century. Theorists such as Antoine-Henry Jomini believed that war could be governed by universal scientific principles, which no doubt appealed to military staff's search for systematic doctrine in the aftermath of the Napoleonic wars. This mechanistic approach emphasised hierarchical structures and defined processes, which in turn influenced early 20th century management theories such as Taylorism.¹¹ Within this paradigm, military commanders and their staff seek to define clear objectives, engineer effects and derive optimal courses of action. Ways and means could be balanced against defined ends using reductionist 'three-column' analysis. In other words, if one does A then B, C is expected to follow. Therefore, contemporary military decision-making frameworks (particularly at the operational and strategic levels) can be considered as a series of sequential steps, decision points and results.

The key to effective decision-making in an adversarial context is tempo, underscoring the value of rapidly cycling through steps to maintain a physical, cognitive and moral advantage – the underlying principle of John Boyd's 'OODA Loop'.¹² The OODA Loop is influenced by Boyd's experience in aerial combat during the Korean War and his experience of combat capability development thereafter. Despite his relatively scant canon, Boyd's theories have influenced 'western' military strategic and operational doctrine for decades.¹³ Boyd's cycle commences by observing, which involves the gathering of information from one's environment. Orientation takes place through analysis and deduction of selected relevant information. Decide involves the determination and selection of a particular course of action. Finally, Act is the implementation of the decision. Those familiar with NATO's Joint Doctrine for Planning Operations (AJP-5) and our own Military Doctrine for the Irish Defence Forces (IRLJP-01) will observe this cycle reflected in our operational design frameworks.

Challenges to Traditional Decision-Making

Decision-making's reliance on predictable cause-effect relationships falls short in dynamic and chaotic contexts, where outcomes are often emergent instead of pre-determined. Complexity has become one of the defining features of our era. Kilcullen describes modern conflict as messy and ambiguous, "shaped more by interactions than individual actors."¹⁴ A complex system comprises many dynamically interacting elements. Humans, by nature are complex systems owing to the substantial number of interactions and the intricate web of causal relationships that occur.¹⁵ A person's orientation to their external environment adapts and evolves through continuous interaction with it and their internal perception of the information they receive about it.¹⁶ With war increasingly taking place "among the people," and particularly enabled through online communication, it begins to resemble a complex adaptive system (CAS) characterised by self-organisation and adaptation to

11 Ben Zweibelson, *Beyond the Pale: Designing Military Decision Making Anew*, (Maxwell Air Force Base: Air University Press, 2023), 154.

12 Cara Wrigley and Murray Simons, *Creativity in Military Complexity: Design, Disruptors and Defence Forces*, 1st ed. (London: Routledge, 2024), <https://doi.org/10.4324/9781003502180>.

13 Ian T. Brown, *A new conception of war: John Boyd, the US Marines, and maneuver warfare*, (Quantico: Marine Corps University Press, 2018), 100; Grant Hammond, *The Mind of War, John Boyd and American Security*, (Washington, D.C.: Smithsonian, 2001)

14 David Kilcullen, *The accidental guerrilla: Fighting small wars in the midst of a big one*. (New York: Oxford University Press, 2011)

15 Lewis A. Coser, (2004). *Masters of sociological thought: Ideas in historical and social context*. 2nd edn. (Rawat, 2004)

16 David J. Bryant, 'Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making', *Military Psychology* 18, no. 3 (2006): 183–206, https://doi.org/10.1207/s15327876mp1803_1.

evolutionary pressures.¹⁷

As AI-enabled information systems take on a greater role in our lives, interpreting the scale of interacting nodes, relationships, and potential risks within a CAS is likely to become increasingly difficult. The challenge for decision-makers is to understand their evolving situation and articulate their objectives, while simultaneously trying to achieve them.¹⁸ Some have likened this reality to playing chess on multiple stacked boards where each move influences the moves of all other boards.¹⁹ Dealing with complexity demands advanced problem-solving capabilities. If military institutions fail to develop such capabilities, they are likely to continue planning and engaging in tactical activities based on outdated models of understanding, misaligned with the contemporary operating environment. In the midst of a similar change moment a century ago, J.F.C Fuller argued that the military's apparent opposition to progress stems not only from its "worship of traditions" but its "incapacity to see world forces in their true relationship".²⁰ In a world increasingly shaped by complexity, adaptability (not linearity) must guide military cognition and command.

'Worship of tradition,' as described by Fuller manifests as a resistance to change and is often rooted in deeper systemic factors. Barnes Wallis (of Dambusters fame), attributed this to a natural opposition among people to anything they have not thought of themselves. An over-reliance on historical precedent as the principle lens for anticipating emerging challenges limits military forces' ability to recognise or exploit novel challenges.²¹ Military leaders are trained to assume a static world where the sequential steps of our planning models remain valid from conception to execution, in other words, preparing to fight the last war.²²

An institutional culture that promotes the development of advanced problem-solving capabilities is enabled by innovation and enhancing diversity of thought - areas our own organisation has actively sought to address. Excluding the perspectives that challenge dominant frames risks limiting the organisation's capacity to respond to events as they arise.²³ Diverse perspectives and appropriate language enable decision-makers to make sense of their world. For example, the success of Project Maven (as outlined above) in helping to defeat ISIS was enabled by its modest, operationally-focused structure empowered to leverage partnerships outside of the military and crowd-source solutions with user communities.²⁴ Inclusivity and innovation are fundamental characteristics of an adaptive culture which when championed from the highest levels and embraced by the organisation can promote agile decision-making and overcome inertia.

Gaining advantage in mosaic warfare requires military decision-makers to do more than just cope with complexity, but to arrive at a situation where systemic interrelations

17 Rupert Smith, *The utility of force: The art of war in the modern world*. (Penguin, 2012); Ben Johnson, "The Age of Disorder," Wavell Room, 09 August 2023, Available at: <https://wavellroom.com/2023/08/09/the-age-of-disorder/>.

18 Stephanie E. Huebner, *Learning to Think for Understanding: Introducing Systems Thinking into Professional Military Education*, School of Advanced Military Studies, US Army Command and General Staff College (2020), 18.

19 Thom Hawkins and Alexander Kott, "Beyond the Hype: Why We're Closer to AI-Enabled Mission Command than You Think," *Modern War Institute*, 04 May 2022, Available at: <https://mwi.westpoint.edu/beyond-the-hype-why-were-closer-to-ai-enabled-mission-command-than-you-think/>

20 Colonel J.F.C. Fuller, *The Foundations of the Science of War*, (Hutchinson & Co., 1926), 31.

21 Zweibelson, *Beyond the Pale*, 207.

22 Johnson, "The Age of Disorder," (2023)

23 Zweibelson, *Beyond the Pale*.

24 Gregory C. Allen, "Project Maven brings AI to the fight against ISIS," *Bulletin of the Atomic Scientists*, 21 December 2017. Available at: <https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/>.

can be perceived and acted on, or as Fuller articulated ‘seeing world forces in their true relationship’. The human mind exhibits an interplay of intuitive impressions and deliberate reasoning, often influenced by the mental models we develop to make sense of the world.²⁵ ‘Heuristics’ are the cognitive shortcuts we use to understand and approach problems, with ‘problem-solution’ being the dominant mode of framing.²⁶ In enacting these shortcuts, we are naturally influenced by our social conditioning and contextual factors. Thus, through our simplification of the world we frequently inject ‘cognitive bias’ to our understanding. Cognitive biases mean we are likely to disregard information that does not ‘fit’ within our established problem-solution frame. When coupled with an over-saturation of information associated with mosaic warfare, biases can lead to ineffective assessments and increased operational risk or failure. A stark example being the failure of Israel’s intelligence apparatus to accurately identify Arab intent in advance of the 1973 Yom Kippur War owing to doctrinal conformity and a lack of institutional challenge.²⁷

While algorithms are capable of harvesting and analysing much larger volumes of data, they are not immune to biases as a result of the inputs and information collected.²⁸ Predictive policing studies in the USA demonstrated how algorithmically-derived decisions generated from biased AI training data sets caused law enforcement officers to disregard contradictory information arising from an evolving scenario.²⁹ A new form of bias in military decision-making is becoming apparent – automation bias. As people ascribe human-like characteristics to machine learning and view it as more capable, they will increasingly use automation as a ‘heuristic replacement’ for verification of information and processing supervision.³⁰ We can see this play out on the social media platform X, in which a ‘chatbot’ known as ‘GROK’ is frequently engaged in the comment sections of user’s posts. Nonetheless, more experienced commanders and staff are likely to continue favouring their own judgement, particularly when they fail to comprehend the processes employed to generate conclusions about the risks and vulnerabilities across the complex system.³¹ Mistrust in the opaque nature of emerging technologies has the potential to stymie wider adoption of technological solutions to mitigate the challenges of a CAS, particularly among key decision-makers. In such a scenario, militaries that do not adopt some form of algorithmic enabler may be walking backwards into the future.³²

Facing the Future Head-On

Preparing military leaders to navigate CAS requires a reflection on how and why we think. When we view the environment as a complex system we begin to understand that there are often initial, secondary and tertiary effects of our decision and actions. Systems thinking offers a lens through which decision-makers can interpret their situation, identify root

25 Daniel Kahneman, *Thinking, Fast and Slow*, (London: Penguin, 2011)

26 Russell L. Ackoff, “On the use of models in corporate planning,” *Strategic Management Journal* 2, no. 4 (1981): 353-359.

27 Noah B. Cooper, *AI and Intelligence Analysis: Panacea or Peril?* War on the Rocks, 10 October 2024, Available at: <https://warontherocks.com/2024/10/ai-and-intelligence-analysis-panacea-or-peril/>.

28 Peter Layton, “Algorithmic warfare: Applying artificial intelligence to warfighting,” (Australian Air Power Development Centre, 2018).

29 Kevin Millar 2014; Albert Meijer and Martijn Wessels 2019 in Johnson, “The AI Commander Problem: Ethical, Political, and Psychological Dilemmas of Human-Machine Interactions in AI-Enabled Warfare,” 214.

30 Johnson, “The AI Commander Problem,” 256.

31 Anna Nadibaidze, Ingvild Bode, and Qiaochu Zhang, *AI in Military Decision Support Systems: A Review of Developments and Debates* (Odense Center for War Studies, 2024).

32 Wrigley and Simons, *Creativity in Military Complexity: Design, Disruptors and Defence Forces*, 102.

causes of problems, and influence the various interacting nodes.³³ Adaptive decision-making cycles have emerged based on a systems thinking approach. At their heart is the above premise that one cannot understand a CAS except by interaction with it. The Australian Defence Forces (ADF) have been at the forefront of this conversation for some years. Bryant's Create, Explore, Compare, Adapt (CECA) and the ADF's Act, Sense, Decide, Adapt (ASDA) models represent an evolution of the OODA Loop in prioritising systemic enquiry and experimentation (sense-making), disregarding the initial observation of Boyd's loop. Both models incorporate iterative feedback loops and focus on emergent stability (adaption) rather than rigid outputs.³⁴ They do not replace the core premise of Boyd's OODA loop but offer alternative perspectives when engaging with complex operational or strategic contexts, in contrast to Boyd's primarily tactical frame.

Enabling adaptive decision-making requires embracing uncertainty and fostering creativity, intuition, and interdisciplinary collaboration. Sensemaking is a critical competency of adaptive decision-making, prioritising plausible understanding over definitive orientation in unpredictable complex systems. Sense-making is developed through discourse and competition with diverging views. It is sustained by intuition and experience enabling decision-makers discern patterns of regularity that can fill the blank spaces of knowledge.³⁵ As such, the competence required for sense-making is largely tacit. Finding the space and language for communicating this is crucial. Regarding adaptability, General Stanley McChrystal made it a central tenet of his leadership in an attempt to optimise his various staffs - not for efficiency, but to embrace uncertainty.³⁶ Adaptability demands a culture that champions creativity and unorthodox thinking in leader development. The Irish Defence Forces' Chief of Staff Innovation Awards and the Defence Forces Review's annual publication are crucial outlets in this regard, but more can be done to engage with public and private sectors.

Enhancing data literacy is critical for decision-makers to effectively lead analysts, navigate the limitations of human-machine interactions, and critically engage with outputs generated by AI.³⁷ Peter Layton notes that cultivating trust in AI systems - anchored in robust ethics, governance, and continuous validation - remains a cross-cutting enabler of wider adoption.³⁸ Skills, such as data science, analytics and visualisation should be encouraged among our personnel to ensure decision-makers possess the correct language and information when making decisions in a data-rich environment enhancing trust in AI-generated outputs. The Defence Forces should prioritise 'explainable AI' in capability generation and personnel development. Dual training of human operators and AI systems in realistic scenarios (known as Human-Machine Teaming) underscores the importance of symbiotic development. The starting point must be adoption.

33 Huebner, *Learning to Think for Understanding: Introducing Systems Thinking into Professional Military Education*, (2020)

34 Bryant, "Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making," (2006); Mike Brennan and Justin

Kelly, "OODA versus ASDA: metaphors at war.[Paper in special edition: The Adaptive Army]," *Australian Army Journal* 6, no.3 (2009): 39-51

35 Andrew D. James, "Emerging Technologies and Military Capability," in *Emerging Critical Technologies and Security in the Asia-Pacific*, ed. Richard A. Bitzinger (Palgrave Macmillan, 2016), https://doi.org/10.1057/9781137461285_2, 5

36 Gen. Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World*, (Penguin, 2015)

37 Alexander Treiblmaier, 'Improving Efficiency Through Data-Driven Decision-Making In A Military Environment', TDHJ, 27 October 2022, <https://tdhj.org/blog/post/data-driven-decision-making-military/>; Nadibaidze, Bode, and Zhang. *AI in Military Decision Support Systems: A Review of Developments and Debates*.

38 Layton, "Algorithmic warfare: Applying artificial intelligence to warfighting."

Given that AI technologies will likely emerge from civilian sectors, agility and responsiveness in our capability development function are critical for leveraging cutting-edge innovations.³⁹ In theory, this should be less problematic for a country as technologically-advanced as Ireland. The Defence Forces should exploit agile, cross-cutting teams consisting of military, academic and civilian stakeholders to rapidly solve problems and promote a wider system of national defence and resilience. The Science Foundation Ireland ‘Defence Organisation Innovation Challenge’ is a good example of cross-cutting teams working to solve defence problems through disruptive technologies. As always, more could be done to widen this initiative and reduce the time from concept to solution thus increasing our agility and responsiveness to emerging challenges.

The generation of a suitably reflexive decision-making ethos hinges not solely on the introduction of new methodologies or technologies, but on the cultivation of a supporting institutional culture that promotes its practice. Professional norms and ethos are shaped and reinforced by our PME institutions giving them a degree of significance in any conversation on culture change.⁴⁰ However, while PME promotes critical thinking, constituent schools rarely educate leaders to understand how their decisions and actions are interpreted and played out in a system.⁴¹ While a deeper examination of PME is outside the scope of this paper, it is argued that the time has come for a pedagogical shift from one based on rote memorisation to one promoting the connection of ideas and creative dialogue.⁴² Alternative analysis methodologies emphasise visualisation and creative techniques to model systemic effects of decisions and foster collaborative, reflective analysis ‘beyond the start line’.⁴³ Alternative analysis techniques can include simple techniques such as brainstorming to more complex methods such as wargaming or alternative futures, all of which are readily enhanced with AI.⁴⁴ Alternative analysis techniques supported by AI tools enable decision-makers to conceptualise the environment as a dynamic system with cascading effects. A recommended start point for our organisation is the adoption and promotion of manual techniques based on realistic scenarios. We must evolve beyond applying unsuitable decision-making frameworks to solve complex problems.

39 James, “Emerging Technologies and Military Capability.”

40 Pierre Bourdieu, *The Logic of Practice* (Polity, 1999), 53.

41 Huebner, *Learning to Think for Understanding: Introducing Systems Thinking into Professional Military Education*, 42.

42 Mark Burnett, Pete Wooding, and Paul Prekop, “Sense Making-Underpinning Concepts and Relation to Military Decision-making,” 9th International Command and Control Research and Technology Symposium, Defence Science and Technology Organisation, Command and Control Division (Australia, 2004).

43 Huebner, *Learning to Think for Understanding: Introducing Systems Thinking into Professional Military Education*; NATO, *The NATO Alternative Analysis Handbook* (Second Edition), December 2017

44 NATO Strategic Warfare Development Command, “Harnessing AI: ACT at the forefront of innovation,” 16 April 2025. Available at: <https://www.act.nato.int/article/harnessing-artificial-intelligence/>.

Conclusion

Relying on a binary perspective of the operating environment, primarily concerned with the components and systems under one's direct influence and control, blinds commanders to the broader strategic picture and evolving dynamic of potential adversaries. While developments in individual technologies and platforms may be evolutionary, their enhancement with AI and exploitation through such as 'exploitation through concepts such as mosaic warfare' may yet prove revolutionary.⁴⁵ Mosaic warfare combines cognitive sciences and advanced technologies to gain advantage over potential adversaries. However, this does not occur without broader institutional change.

This paper has argued for a shift from industrial-age mechanistic decision-making to one postured for complexity. We can no longer expect conditions to remain static while we observe and orientate to the realities of our operating environment. Additionally, we should no longer engage in decision-making frameworks such as MDMP and OPP expecting confirmation of our belief regarding how modern warfare *ought* to function.⁴⁶ The adversary, of course, always gets a vote. Shifting mindsets and developing the competencies of sense-making and adaptability begins with an organisational culture that is suitably reflexive to encourage challenge and innovative thinking. Drawing again on Gen Stanley McChrystal, organisations that continue to use 20th century tools in today's complex environment do so at their peril.⁴⁷ If Óglaigh na hÉireann expects to be a joint, agile and fit-for-purpose military force it begins with a shift in mindset to one postured for the realities of modern warfare.

⁴⁵ James, "Emerging Technologies and Military Capability," 3.

⁴⁶ Ben Zweibelson, *Beyond the Pale*, 76.

⁴⁷ McChrystal, *Team of Teams: New Rules of Engagement for a Complex World*.



Maintaining Ethical Leadership in Grey Zone Operations

Dr Dennis Vincent MBE

Introduction

Operating in the grey zone against hybrid threats present new challenges to military leaders and increases the pressure on them to make challenging decisions in ambiguous and volatile situations. Grey zone operations are ‘multi-dimensional activities aimed to alter adversary behavior [sic] while remaining below the threshold of conventional military employment.’¹ A good example of grey zone operations was the Russian military actions in Crimea and eastern Ukraine ahead of their invasion in 2014. The requirement to act positively in volatile, uncertain, complex and ambiguous situations can cause additional stress on leaders. Unless they are aware that their cognitive ability will be degraded and their behaviour altered, they may not respond in an authentic and values-based way.

This article will investigate how the practical application of authentic, ethical leadership is conducted using the S-CALM Model.² The acronym S-CALM stands for: Situational Influencers, Common Behaviours, Accountability, Leadership and Moral Compass. The S-CALM Model provides a simple toolkit that acts as a handrail for ethical decision-making when leaders are confronted with the emotions and stresses of command in ambiguous grey zone operations. This article will outline the S-CALM Model in two sections. The first section explains why leaders make unethical decisions under stress. It will explore three components: firstly, historical research which reveals how the power of the situation has an influence over people and is stronger than their character or will. The second component explores the situational influencers in the contemporary operating environment that enhance the power of the situation. The five common situational influencers identified are ‘hostile environment, normalised violence, weak leadership/lack of supervision, lack of resource/fatigue and enhanced emotional state.’³ The final component this section will describe how under the enhanced power of the situation, people change the way that they behave. It outlines the twelve common behaviours in military organisations that are displayed in grey zone situations. The second section will briefly illustrate how a leader can cope with these behaviours in a stressful situation by using the S-CALM Model.

Why Unethical Actions Happen in the Grey Zone?

Unlike normal military campaigns, there are no clear behavioural rules within grey zone operations. My research has found that in these situations, there are three considerations, the first of these is unethical activities start with small actions which then escalate. This phenomenon is termed by the International Committee of the Red Cross (ICRC) as ‘The Spiral of Violence.’⁴ The second consideration is termed ‘The Banality of Evil.’⁵ It contends that the ability to conduct evil, unethical acts is within

1 Tahir Mahmood Azad, Muhammad Waqas Haider, and Muhammad Sadiq, “Understanding gray zone warfare from multiple perspectives,” *World Affairs* 186, no. 1 (2023): 84.

2 Dennis Vincent. *The S-CALM Model: The Application of Ethical Leadership in the Military* (Havant: Howgate Publishing, 2025).

3 *Ibid.*, 3.

4 ICRC, *The Roots of Behaviour in War: Understanding and Preventing IHL Violations* (Geneva: ICRC, 2004), 16.

5 Hannah Arendt, *Eichmann in Jerusalem: A Report on the Banality of Evil* (New York: Viking Press, 1963), 276.

everyone and not just a few evil people. The final consideration is known as ‘The Power of the Situation.’⁶ This final concept is the most important as it asserts that under the pressure of a stressful situation individuals and teams behave in ways driven by the environment itself, which is more powerful than their characters and beliefs. It is this power of the situation which is particularly strong in the unregulated grey zone environment.

There are certain influences that enhance the power of the situation and result in non-values-based behaviour in grey zone operations. Defence Force Leadership Doctrine states that ‘leaders must be aware that biases, fatigue and stress can influence thought’ and these are important.⁷ However, my recent research has identified five common ‘Situational Influencers’ which can enhance the power of the situation:

- **Hostile Environment.** A hostile environment is one in which a person feels under threat due to the perception of danger. People tend to act differently in a hostile environment than they would if they do not perceive a threat. This point is intricately linked to normalised violence below, in that the longer that people are exposed to a hostile environment the more it becomes the social norm and there is moral disengagement. This detachment is often referred to as ‘Ethical Drift’.⁸
- **Normalised Violence.** Everyone has exposure to violence at some level, but for most people this tends to be infrequent, low-level acts. However, if people are exposed to constant violence, it is soon accepted as the social norm and it takes increasing levels of aggression to register as acts of violence. In intensely violent environments, people become immune to the brutality around them and the threshold of inflicting pain on others is lowered.⁹
- **Weak Leadership and Lack of Supervision.** Weak leadership is normally seen when a leader uses a laissez-faire, hands off style with a team that needs to be given more guidance and direction. However, it can also be that the leader is micromanaging their team and followers feel they have no responsibility for their actions. Weak leadership can result in leaders displaying the incorrect level of supervision, which can lead to incremental ethical drift.¹⁰
- **Lack of Resources and Fatigue.** In many situations, leaders believe they do not have the correct level of resource to complete the task. The two key resources lacking tend to be time and people. Leaders who do not have enough time to do things as they should are inclined to prioritise what actions they are able to achieve in the limited time given. Similarly, when leaders do not have enough people to conduct actions as they would have wanted, corners are cut to meet outputs. This deficiency of people and time invariably leads to fatigue amongst those in teams. Furthermore, as the human body requires eight hours sleep a night to regenerate, prolonged periods of less than this reduces cognitive

⁶ Phillip Zimbardo, *The Lucifer Effect: How Good People Turn Evil* (Croydon: Rider Books, 2007).

⁷ Irish Defence Forces, *Defence Forces Leadership Doctrine* (Dublin: Defence Forces Printing Press, 2023), 54.

⁸ Vincent, *The S-CALM Model*, 20.

⁹ *Ibid.*, 22.

¹⁰ *Ibid.*, 24.

ability. Leaders and teams who lack sleep make poor cognitive decisions.¹¹

- **Enhanced Emotional State.** In stressful situations where people experience intense emotions, their ability to do the right thing is often reduced and their judgement can be clouded. These emotions are sometimes referred to as arousal, the common military arousals are anger, rage, frustration and disgust.¹²

Although these five common situational influencers have been presented as separate items, they are in fact more complex than this and there is a large degree of overlap between them. For example, a person who is fatigued is more likely to be in an enhanced emotional state. This interlocking and overlapping complexity is demonstrated in figure 1 below:



Figure 1: Situational Influencers.

My research has shown there are a number of common behaviours demonstrated by those operating under the power of the situation in the complex contemporary operating environment. The behaviours in themselves are not unethical, but in the wrong situation they can lead to non-values-based, unethical behaviour taking place. There are six common individual and six common group behaviours. Starting with the individual behaviours:

- **Social Comparison and Conformity.** These two theories have been grouped as for most people they produce similar behaviours and actions. The definition of social comparison occurs when individuals compare 'behaviours and opinions with those of others in order to establish the correct or socially approved way of thinking and behaving.'¹³ Conformity is defined as a change in 'deep-seated private and enduring behaviour and attitudes due to group pressure.'¹⁴ Here there is a strong social obligation to conform, and this is often termed as peer pressure.
- **De-individuation.** De-individuation is defined as the 'process whereby people lose their sense of socialised individual identity and engage in unsocialised,

¹¹ Ibid., 27

¹² Ibid., 31.

¹³ Michael Hogg and Graham Vaughan, *Social Psychology*, 7th Ed. (Harlow: Pearson, 2014), 664.

¹⁴ Ibid., 658.

often antisocial behaviours.’¹⁵ In simple terms this behaviour sees individuals, especially those in the military, lose their identity to the group.

- Obedience. Obedience is defined as a ‘behaviour in compliance with a direct command, often one issued by a person in a position of authority.’¹⁶
- Cognitive Dissonance. Cognitive dissonance can be thought of as a ‘state of psychological tension produced by simultaneously having two opposing cognitions.’¹⁷ When this occurs, people try to seek harmony between their beliefs and behaviours and attempt to reduce tension that this inconsistency causes.
- Bystander Effect. The bystander effect is defined as the concept where ‘people are less likely to help in an emergency when they are with others than when alone. The greater the number, the less likely it is that anyone will help.’¹⁸ One of the main drivers for this concept is what is known as the ‘Diffusion of Responsibility’ which is the ‘tendency of an individual to assume that others will take responsibility.’¹⁹
- Status Quo Bias. Status quo bias is defined as ‘doing nothing or maintaining one’s previous position.’²⁰ It is often seen when leaders display an unwillingness to change what is established and has worked before.

The six common group behaviours are:

- Groupthink. Groupthink is defined as ‘a mode of thinking in highly cohesive groups in which the desire to reach a unanimous agreement overrides the motivation to adopt proper rational decision-making procedures.’²¹ With groupthink, no one wants to be the first to challenge a decision even if they consider it to be wrong.
- Risky Shift. Risky shift is defined as the ‘tendency for group discussion to produce group decisions that are more risky than the mean of members pre-discussion opinions.’²²
- Authority Bias. Authority bias has been defined as ‘the tendency of people to blindly follow the advice, suggestions, or instructions of others who are in positions of authority.’²³
- Dehumanisation. Dehumanisation is defined as the process of ‘stripping people

¹⁵ Ibid.

¹⁶ APA Dictionary of Psychology. <https://dictionary.apa.org/obedience>

¹⁷ Hogg & Vaughan, *Social Psychology*, 657.

¹⁸ Ibid.

¹⁹ Ibid., 658.

²⁰ W. Samuelson & R. Zeckhauser. “Status Quo Bias in Decision Making,” *Journal of Risk and Uncertainty*, 1, (1988): 8.

²¹ Hogg & Vaughan. *Social Psychology*, 660.

²² Ibid., 663.

²³ Newristics. Authority Bias. Heuristic Encyclopaedia. <https://newristics.com/heuristics-biases/authority-bias>

of their dignity and humanity.’²⁴ The ICRC state that ‘the humanity of the other side is denied by attributing to the enemy contemptible traits, intentions and behaviours.’²⁵

- Othering. Othering is defined as ‘transforming a difference into otherness so as to create an in-group and an out-group.’²⁶ This differentiation between the in-group (‘us’) and the out-group (‘them’) is common in many militaries, which are very quick to assign stereotypes.
- Demonisation. Demonisation is defined ‘as the characterization of individuals, groups or political bodies as evil.’²⁷ In the grey zone ‘there can be the temptation to believe that ‘all we do is good’ and ‘all they do is bad’, intentions and actions become black and white. But combat is never black and white it is always a shade of grey.’²⁸

In the stress of complex, grey zone operations the power of the situation builds and is enhanced by the situational influencers which in turn cause all or some behaviours described here to take place. This flow of activity leads to unethical acts.

The S-CALM Model

The S-CALM Model is a toolkit which provides the means to counter with the flow of unethical actions and is outlined in figure 2. The ‘S’ stands for situational influencers and is a reminder that the power of a situation is enhanced by these five common influencers. Some, such as a lack of resource, might be identified before the situation whilst others, such as enhanced emotional state are likely only to be recognised once emerged in the environment. In a similar vein, the ‘C’ relates to the twelve common behaviours. Leaders must know themselves well to be able to detect a change in their behaviour. Nevertheless, if leaders can identify that they are already susceptible to a certain behaviour before they are placed under stress, they can be prepared to mitigate it when under the pressure caused by situational influencers. Leaders also need to understand the group behaviour of their teams. This allows them to identify the six common group behaviours and prepares them to steer their teams away from unethical actions, even under the stress and ambiguity of grey zone operations.

²⁴ Hogg & Vaughan. *Social Psychology*, 658.

²⁵ ICRC. *The Roots of Behaviour in War*, 10.

²⁶ J. F. Staszak, “Other/Otherness,” *International Encyclopaedia of Human Geography*, 1, (2008): 1.

²⁷ G.O. Faure, “Negotiating with Terrorists: A Discrete form of Diplomacy,” *The Hague Journal of Diplomacy*, 3, no. 2, (2008): 193.

²⁸ Vincent, *The S-CALM Model*, 68.



Figure 2: The S-CALM Model.

The 'A' relates to accountability. In the military there are four types of accountabilities: hierarchical, professional, legal and political. Hierarchical accountability is the default for most military organisations, with responsibility being held by the chain of command and subordinates being accountable to their superiors. Professional accountability is the benchmark that we hold ourselves to in an occupation. In the military this tends to happen when a generalist manager is responsible for a group of subject matter experts. Legal accountability relates to operating within Irish Law and International Humanitarian Law. Whilst political accountability may not seem applicable to most leaders at the junior level. In the age of the 'Strategic Corporal' ensuring that the actions of all members of the team are appropriate is vital.²⁹ This is because even small unethical acts distributed on social media can have national or international impact. The main issue with these four distinct types of accountabilities is that they can conflict with each other and the leader needs to balance them. The British Army Standards are designed to ensure that all individual and group behaviours are accountable and provide a useful handrail in volatile situations. The three Standards are: lawfulness, appropriate behaviour and professionalism. These standards provide a useful checklist for measuring accountability. Therefore, the first question that a leader should ask themselves in a stressful, ambiguous situation is: **Are my actions lawful, appropriate and professional?**

The 'L' in S-CALM is for leadership. Leaders must be courageous in their decision making, and consistent in their supervision, attitudes and activities, to build trust and mutual respect with their teams. To achieve this, leaders in grey zone operations, need to reflect on two considerations in their command, leadership and management responsibilities. Under command, the first consideration is the requirement to demonstrate the loneliness of command. There will be times when the leader will feel under considerable pressure to conform to the group, but Defence Force Leadership Doctrine states that 'commanders alone must always bear responsibility for mission success or failure.'³⁰ If a leader can

²⁹ Charles Krulak, *The Strategic Corporal: Leadership in the Three Block War: Operation Absolute Agility* (Center for Army Lessons Learned, Fort Leavenworth, 2002).

³⁰ Irish Defence Forces, *Defence Forces Leadership Doctrine*, 34.

maintain the condition where they are 'in' the team but not 'of' the team they will be able to manage the required psychological separation. This separation allows a successful leader to make difficult, ethical decisions when the rest of the team want to take easy, unethical actions. This difficult test of leadership is when the concept of the loneliness of command comes into its own. On the second command consideration, few leaders commission unethical acts, but more tend to allow them to happen by omission and do not step in to stop the spiral of violence from taking place. There are two leadership considerations, the first is the requirement to set the moral tone and be the exemplar. The second is the need to gain trust. Trust in the leader is a central commodity. It is vital that followers trust their leaders' abilities and have confidence in their ethical decision-making in complex environments. It can be achieved by a leader demonstrating emotional intelligence and having empathy with their teams. In management, a leader firstly has an obligation to set out their expectations of the team by creating an ethical vision and giving a clear intent to avoid vagueness of understanding. US Army Doctrine states that 'leaders should not intentionally issue vague or ambiguous orders or instructions to avoid responsibility.'³¹ Secondly, leaders are required to ensure that these expectations are achieved by the application of rewards and punishments to motivate the required behaviour in the team. Therefore, the second key question that a leader must ask themselves is, **Do I need to apply the Loneliness of Command?**

Finally, the 'M' is for the moral compass. Most Western militaries use virtue ethics as the mainstay of their moral belief system. Virtue ethics are not focused on a single act, but with the development of a person's character over a longer time. The Defence Forces Values are virtue ethics. When these Values are deep seated in an individual, they become their own personal values and are termed their moral compass. Having a moral compass that points true and displaying moral courage in difficult conditions are vital qualities for ethical leaders. A leader with a strong moral compass is expected to act virtuously whatever the circumstances and external pressure, especially in a complex operating environment. It can be summarised as being able to do the right thing on a bad day when no one is looking. To do this, virtuous ethical behaviour needs to become a leader's intuitive way of thinking and operating. Therefore, the third question that a leader should ask themselves in a stressful, uncertain situation is, **Am I doing the morally right thing?**

³¹ US Army, *ADP 6-22: Army Leadership and The Profession* (Department of the Army, 2019), 2-7.

Conclusion

The complex grey zone operating environment is ‘characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks.’³² In this environment it can be easy to slip into believing that the normal rules of war do not apply and succumb to ethical drift. However, my research has shown that leaders need to identify that they are in a stressful, ambiguous and volatile situation which is having power over way that they and their team both think and act, before it leads to non-values-based behaviour. Once they have recognised this power, they can consider the situational influencers and common behaviours that are influencing them and their team. They can then mitigate this power by asking the accountability, leadership and the moral compass questions. In this way, the S-CALM Model is a useful toolkit for maintaining authentic, ethical leadership under the stress of operating in the grey zone. To understand the S-CALM Model in more depth and see how it relates to real world examples the following book is recommend further reading: **The S-CALM Model: The Application of Ethical Leadership in the Military.**

³² Patrick Bratton, “The Not so Gray Zone in South Asia,” *Comparative Strategy*, 39, no. 1, (2020): 42.



Harnessing the Power of Story: Inoculating the Force Against 'Grey-Zone' Effects

Commandant Tadhg O'Donoghue



Introduction

Storytelling in the Irish Defence Forces (DF) is a contact sport, constituting friendships, neural networks and negotiations of meaning that represent assimilation into groups and socialisation into the wider organisation. Stories represent the “coin and currency”¹ of the culture that military leaders operate in. This paper argues that the DF has an opportunity to harness the power of story to address problems, including an increasingly contested ‘truth-space’ and the malevolent effects of disruptive grey-zone activities. A deeper consideration of story presents the possibility of inoculating the force against hybrid effects and contributing to organisational and broader societal resilience. As the force re-organises and delivers cultural change, an understanding and chronicling of the stories of the DF can contribute to the articulation of a shared future and reinforce the organisation’s values while retaining authentic leadership at the core of its delivery. This paper highlights three opportunities for the DF: the chronicling of organisational stories to anchor core values, a renewed focus on the skills of storytelling for leaders in Professional Military Education (PME) to bolster their authentic register, and the adoption of useful fiction to inoculate the force against grey zone effects.

¹ Jerome S Bruner, *Making Stories : Law, Literature, Life* (New York: Farrar, Shaun, Giroux, 2002).

The Case for Storytelling

"For millennia, humans have gathered to drink from the well of story."²

Storytelling is a powerful social phenomenon that circumscribes our social reality. At a macro level, stories are carriers of collective and institutional memory and culture. At the micro level, stories are woven into human interaction and personal sensemaking. A story invites us on a journey of meaning-making. Hsu outlines the capacity of storytelling to appeal to emotions and our capacity for empathy, highlighting the "narrative transport" that is experienced when a story lands.³ This power of empathy as a response to storytelling informs what a good story must achieve: the power to trigger an emotional response. The curiosity factor must also be considered: how someone opens a story immediately attracts engagement or it doesn't. Contemporary public speaking gurus promote the concept of 'start with a story', the power of the 'five-second moment',⁴ and Campbell's 'heroes' journey' model.⁵ Hsu, examining the evolutionary advantages of storytelling, points out that it improves social cohesion and is an intergenerational carrier of knowledge.⁶ This aligns with the concept of organisations being propped up by a story, for instance, the 'Apple story'.⁷ Strong organisations have a strong story that articulates their 'big why'.

Storytelling is a common feature of professional life; the term 'spinning dits' is a common colloquialism in the UK Armed Forces, as is 'spinning a yarn' or 'aon scéal' in the Irish context. Snowden et al explain that "human society evolved using narrative as a means of creating meaning and communicating knowledge within a network of families, clans and tribes."⁸ To engage in storification (the art of making your point through a story) is to enter a particular modality. There are stories that we generate as part of our sense-making process, but there are also the stories that are inherited: set-piece narratives that are handed on as part of assimilation into a group. These can be referred to as organisational stories.

Ultimately, storytelling harnesses fiction and is predicated on an expected and accepted license to embellish. An enquiry into the nature of storytelling can reveal heuristic limitations. A 'willing suspension of disbelief' is mutually acknowledged in the transaction of stories; often signified by a shift in tone or body language as the person enters 'story-mode'. In military culture, this can be referred to literally and figuratively as a 'take off the beret' (cap/lid) moment, signifying that the teller is speaking 'off the record'. Stories are ever-present in the social dynamics and meaning-making experiences of people as they understand the 'truths' of their experiences.

2 Martin Shaw, "The School of Mythopoetics," *The School of Mythopoetics*, 2024, <https://www.schoolofmythopoetics.com/>.

3 Jeremy Hsu, "The Secrets of Storytelling," *Scientific American Mind* 19, no. 4 (August 2008): 46–51, <https://doi.org/10.1038/scientificamericanmind0808-46.47>.

4 Matthew Dicks, *Storyworthy: Engage, Teach, Persuade, and Change Your Life through the Power of Storytelling* (New World Library, 2018).

5 Joseph Campbell, *The Hero with a Thousand Faces* (Mumbai, India: Yogi Impressions, 1949).

6 Jeremy Hsu, "The Secrets of Storytelling".

7 Matthew Syed, *Rebel Ideas: The Power of Diverse Thinking*. (S.L.: John Murray Publishers, 2019). 162.

8 David Snowden and Cynthia Kurtz, "Bramble Bushes in a Thicket Narrative and the Intangibles of Learning Networks," *The Cynefin Co.*, 2000, <https://cdn.cognitive-edge.com/wp-content/uploads/sites/2/2020/11/16123947/52-Bramble-Bushes-in-a-Thicket-1.pdf>. 21.

Storytelling and Leadership

Military leaders tell stories, have stories told about them, and pay homage, consciously and unconsciously, to organisational stories. In engaging with story, the leader's role is not necessarily to reflect the outward appearance of things but rather the inner significance of organisational events, helping their audience make meaning for themselves. The journey of the leader from induction to eventual command is one of developing literacy in the key knowledge assets of their organisation and inviting others to participate in a deeper understanding of why they must do what they do. The authenticity of the register ultimately decides the extent to which the leader is deemed to be worthy of following. Paradoxically, a leader's story need not be factually true to tell organisational truths. The utility of story is in the opaque relationship it can have with ontological truth. Its art lies in holding a mirror up to reality and offering the listener a way to the truth through engagement with the story. The US General, Jim Mattis, in describing his leadership style, explained that he "*used touchstones . . . leavened with history's enduring lessons.*"⁹ This illustrates the power of persuasion available to the skilled storyteller.

In a contested truth space, having received the commander's intent, subordinates will have access to alternative narratives describing the operating environment on their personal devices, which they must negotiate, understand, and tell their own truth. Narrative skills saturate the Information Domain, requiring the military commander to develop antennae to understand adversary ways and effectively counter through a compelling narrative. Military leaders can develop their story and their storytelling skills. Snowden speaks about "*spotting the micro-stories or street stories that indicate a ground swell for change.*"¹⁰ This highlights the role of military leaders as anthropologists. A leader can only effectively tell a good story if they are students of contextual stories in their environment. Understanding atmospherics through the tone and undercurrent of the stories being transmitted in the localized system is an anthropological skill that the leader can benefit from. Here, coaching can offer a significant development benefit, specifically modalities and techniques such as narrative coaching and cognitive behavioral coaching.¹¹ This can have a cathartic impact on leaders, particularly at moments of transition in their careers, such as taking over a command role.

In such a new-normal world, authentic leadership has never been as challenging or as critical to operational capability. Maya Angelou said that "*people will forget what you said . . . but will never forget how you made them feel.*"¹² The military storyteller is best concerned with displaying how much they authentically care before leveraging how much they know. Developing an awareness of situational and dispositional factors assists the leader in developing this judgement. Taking the time to acknowledge and understand the stories of others is a powerful act of empathy, demonstrating how much the leader cares. The stories

9 Jim Mattis and Bing West, *Call Sign Chaos: Learning to Lead* (New York: Random House, 2019), 239.

10 TEDx Talks, "Discussion on the Cynefin Framework | Dave Snowden & Imre Porkoláb | TEDxBudapestSalon," *YouTube*, May 11, 2020, https://www.youtube.com/watch?v=_waoADNcaBU.

11 David Clutterbuck, *Coaching the Team at Work* (New York: Nicholas Brealey Publishing, 2011).

12 Maya Angelou, "A Quote by Maya Angelou," Goodreads.com, 2019, <https://www.goodreads.com/quotes/5934-i-ve-learned-that-people-will-forget-what-you-said-people>.

of the very small can be reframed as a microcosm of the stories of the very big and generate shared understanding and more powerfully, a co-created meaning-making context.

Parry and Hansen contend that effective stories have a moral dimension that represents the 'authenticity' of the story¹³. Though moralizing is not an attractive quality in a leader, a military leader should consider what message of morality is implicit in a story that is being told. A leader's situational awareness and ego is critical to their relationship with story. For instance, French and Simpson examine the motivations and effects of leaders that downplay their leadership role.¹⁴ Audiences, military or otherwise, are unimpressed by narcissists who only tell stories about themselves. In recounting personal anecdotes, a confident but post-heroic register is optimal.

Developing Storytelling Leaders

The military leader should seek to develop and maintain a neural network that sustains diverse story acquisition to broaden their meaning-making context. The compelling storyteller can reach into diverse areas to recruit motifs and reveal patterns that increase the number of meaning-making 'hooks' available to the follower. Snowden argues that innovation is only achieved through placing people in situations of cognitive stress.¹⁵ As such, storytelling can provide a training platform to project military leaders into situations where they examine their response to the problem set of the story. Parry and Hansen suggest a focus on "building better stories just as much as . . . building better leaders"¹⁶ and Gaines outlines the benefits of storytelling training in the US military.¹⁷ At a basic level, knowledge of the dynamics of story from critical theory can elevate the leader's ability to communicate and 'sell' the commander's intent.

The military leader who has a story for every situation can be a powerful actor in an organisation. Stories can be used to prepare followers for difficult future situations. Knowledge of story can augment military training in areas such as induction, leadership and career advancement training, as well as red-teaming in operational planning. Brown explores the utility of storytelling in the context of military education in the US Armed Forces.¹⁸ This highlighted that where instructors' stories revealed vulnerability as part of cautionary tales, they landed best. However, stories that were overly self-deprecating damaged the instructors' effectiveness.¹⁹ A further conclusion of this study was that students resisted stories that were closed in their decision-making. This suggests that students prefer to engage with instructor stories as a co-creationary process. Gaines and Fletcher outline a 'pathway' for leaders in how they can incorporate storytelling, characterising a commander's intent

13 Ken W. Parry and Hans Hansen, "The Organisational Story as Leadership," *Leadership* 3, no. 3 (August 2007): 292, <https://doi.org/10.1177/1742715007079309>.

14 Robert French and Peter Simpson, "Downplaying Leadership: Researching How Leaders Talk about Themselves," *Leadership* 2, no. 4 (November 2006): 469–79, <https://doi.org/10.1177/1742715006068936>.

15 TEDx Talks, "Discussion on the Cynefin Framework | Dave Snowden & Imre Porkoláb | TEDxBudapestSalon."

16 Parry and Hansen, "The Organisational Story as Leadership," 293.

17 Tom Gaines, "Stories That Win Wars: The Role of Narrative in Military Planning and Innovation - from the Green Notebook," *From the Green Notebook*, December 2, 2024, <https://fromthegreennotebook.com/2024/12/02/stories-that-win-wars-the-role-of-narrative-in-military-planning-and-innovation/>.

18 Lisa G Brown, "Storytelling as an Instructional Technique: Recommendations for Military Instructors," (Dissertation, 2021), <https://www.armyupress.army.mil/Journals/Journal-of-Military-Learning/Journal-of-Military-Learning-Archives/October-2022/Military-Instructors/>.

19 Ibid. 66.

as “the simplest possible story of what must be done and why.”²⁰ A skilled storyteller has significant advantages as a leader. Stories represent a social contagion and are a predictor of the reception that a leader will receive from followers.

Organisational Stories

Organisations present their stories through lore, tradition, commemoration, rituals and objects. The phenomenon of sacralisation, the act of making something sacred, can describe military traditions of rituals that provide identity touchpoints and anchor the process of military socialisation and indoctrination. Similarly, stories function as these touchpoints and can undergo the phenomenon of sacralisation. Stories in organisations are subject to social contagion: they multiply and proliferate throughout the organisation with each retelling.²¹ Terms like “rumour mill” refer to the social contagion of often toxic stories that undermine the organisation’s integrity. Caforio highlights the place of tradition, history and rite of passage in the storytelling role of the military manager.²² That stories are unstable and evolving is clear. This can be understood as a literary Darwinism; stories develop to meet the needs of the population. Stories that ‘stand the test of time’ in organisations can be likened to be ‘itinerant objects’; understanding objects as having an itinerary which helps us “fully consider their present entanglements as central to their story”.²³ Viewing stories as ‘itinerant objects’ (like the story referred to in comic strip form at above) allows us to chart cultural transitions in organisations. This presents the idea of story as a mirror placed before an organisation, continuously revised and co-created between the organisation, the leader group, and the follower group.

Harris and Barnes outline effective storytelling techniques and themes with specific utility for leaders in business, and question the use of experience if it cannot generate a well of stories that, through skill acquisition can be mobilised towards constructing collective organisational meaning and effecting change.²⁴ Members that identify with organisations enter into the stories of that organisation, breathing oxygen upon the embers of organisational narratives. The DF Leadership Doctrine (DFLD) canonises organisational stories through 15 vignettes. The use of doctrine to socialise organisational stories is not without precedent and is a prominent feature of the British Army’s equivalent document.²⁵ However the British Army further seize upon the power of story when they indoctrinate cadets by issuing them with a chronicle of stories and reflections collected in *Serve to Lead*.²⁶ Snowden and Kurtz warn against the dangers of organisational storytellers.²⁷ This paper highlights how overtly choreographed stories can foster cynicism and toxic anti-stories. It suggests that organisations must recruit stories from the ground up and avoid the potential pitfall

20 Tom Gaines and Angus Fletcher, “The Commander’s Path to Victory: Communication without Comms,” *Modern War Institute*, October 17, 2023, <https://mwi.westpoint.edu/the-commanders-path-to-victory-communication-without-comms/>.

21 Parry and Hansen, “The Organisational Story as Leadership,” 293.

22 Giuseppe Caforio, “Rhetorical Persuasion and Storytelling in the Military,” in *Armed Forces, Soldiers and Civil-Military Relations* (Wiesbaden: VS Verlag Fur Sozialwissenschaften, 2009), 89–99.

23 Alexander Bauer, “Annual Review of Anthropology Itinerant Objects,” *Annual Review of Anthropology* 48 (2019), 336, <https://doi.org/10.1146/annurev-anthro-102218->.

24 Jack Harris and B. Kim Barnes, “Leadership Storytelling.”

25 UK Armed Forces, ‘Army Leadership Doctrine AC 72029,’ 2015, https://www.army.mod.uk/media/24335/20210923_army-leadership-doc-trine-web_final.pdf.

26 UK Armed Forces, ‘Serve to Lead,’ *Army Cadet Force Resources* (Sandhurst: Army Cadet Force Resources, 1947), <https://www.mkbartlett.co.uk/data/further/0311MOJFR01.pdf>.

27 Snowden and Kurtz, “Bramble Bushes in a Thicket,” 13.

of editorialising to speak about values. Here, the DFLD (and more so the British Army Leadership Doctrine) is strong; it gives voice to the protagonists and represents their stories in their own words rather than editorialising. Where stories are canonised, the editorial signature of the organisation must be minimal.

Organisational stories turn up in the internal negotiation of conflict. Snowden and Kurtz interrogate how narrative participates in the network effects of identity, trust and conflict, explaining how we use narrative reasoning to understand and negotiate conflict.²⁸ This highlights the “dangers when one uses narrative without adequate attention to the unique qualities of stories as communicative devices”.²⁹ In a contested truth environment stories that are elevated to doctrinal publications and become touchpoints for meaning-making, instructing members as to how the organisation negotiates and responds to conflict.

Stories that do the rounds in the barrack rooms reveal the values and shadow values of organisations. However, stories that are canonised through chronicle can reinforce (or become) the anchor for an organisation's values. *Serve to Lead* in the British context evidences the values that leadership would have new entrants espouse to. It provides touchpoints from history and offers role models to aspiring leaders and storified actors that embody the organisation's values. Moreover, it assures the reader that they are entering into a greater culture of values-based leadership, into a greater story that they are invited to contribute to.

Useful Fiction as Inoculation

Contemporary militaries are seizing on the power of storytelling through ‘useful fiction’.³⁰ Singer identifies how the stories of useful fiction help “draw upon lessons of the past while imagining the future”.³¹ Useful fiction evidences a recognition that stories can prepare organisations for their future.³² It is an opportunity for an organisation to present the autobiographical story that it wants to share about itself and its future. Stories can function as carriers of organisational values. The DFLD highlights stories that are elevated to doctrine and epitomize what the organisation means when it talks about its values and leadership. Useful fiction can be recruited to prepare the forces for the grey zone activities that are likely to be waged against Ireland in the future and storify the DF members that will respond to these challenges. Useful Fiction can present the characteristics and implications of a disruptive post-truth environment and, as such, serve as an inoculation to such effects and bolster national resilience. As the West, at the time of writing, contemplates the re-emergence of symmetric, state-on-state warfare on mainland Europe, it is worth considering the effect of the canon of stories that are mainstreamed. Europe's existential threat, Russia, conducts statehood and war in a classical, heroic manner. Pluralist Ireland (and perhaps Europe), conversely, is distinctly post-heroic, canonising stories that valorise elevated understandings of higher-order concepts such as the indirect approach and ethics. Useful fiction can now be recruited by the DF to prepare leaders for the distinct generational leadership challenges that represent the new normal, contested truth, operating environment.

²⁸ Ibid. 18.

²⁹ Ibid. 20.

³⁰ Jonathan Klug, Steven Leonard, and Mick Ryan, *To Boldly Go: Leadership, Strategy, and Conflict in the 21st Century and Beyond* (Havertown: Casemate Publishers & Book Distributors, LLC, 2021).

³¹ August Cole and P W Singer, *The Fourth Age: The Future of Special Operations* (Joint Special Operations University, 2023). A005.

³² Ben Quinn, “UK Ministry of Defence Enlists Sci-Fi Writers to Prepare for Dystopian Futures,” *The Guardian* (The Guardian, January 19, 2025), <https://www.theguardian.com/uk-news/2025/jan/19/ministry-of-defence-enlists-sci-fi-writers-to-prepare-for-dystopian-futures>.

Opportunities for the DF

Stories and storytelling represent a powerful and often overlooked phenomenon in organisational culture. Leaders mobilise stories, with varying degrees of skill, to communicate their intent. Leaders reflect upon the stories that form their professional identity as they negotiate how their narrative maps onto organisational stories. Stories represent the “coin and currency”³³ of the DF's organisational culture.

Based on the ideas and literature presented above three opportunities for the DF emerge. The DF should now acknowledge and develop storytelling skills as part of leadership education on PME courses supporting leaders in developing their authentic leadership register. The organisation can further support this by maintaining and broadening the formal coaching offering to leaders at all levels to develop understanding of narrative and the place of story in their leadership journey and output.

It is timely that the DF chronicles organisational stories in the model of the British Army's *Serve to Lead*. This will benefit the organisation in reclaiming stories as itinerant objects that function as carriers of the values of the organisation and mobilising story towards organisational socialisation and cultural change. Additionally, consideration should be given to the reorientation of the next edition of the DFLD towards narrative forms that consider generational problem sets.

Finally, the DF can now consider investment in useful fiction to storify the future and inoculate the force against the grey zone effects that represent the new normal in the contemporary operating environment. Useful fiction can provide the platform upon which the organisation, its members and the society it represents can negotiate and ultimately ‘tell the story’ of the shared future of the defence of Ireland.

33 Jerome S Bruner, *Making Stories: Law, Literature, Life*, 16.



Bridging the Generational Gap: Leading Gen Z and Gen Alpha in the Post-Truth Era

Sergeant Stephen McCabe

Introduction: A Generational Turning Point

The Irish Defence Forces (DF) are undergoing a period of significant transformation. This shift is driven by the Government's commitment to modernise capabilities, enhance readiness, and adapt force structures in line with emerging security challenges, as outlined in the *Defence Policy Review 2024*.¹ While structural reforms and geopolitical uncertainty draw institutional focus, a quieter yet equally critical shift is occurring: the changing character of the personnel who serve. Recruits today, drawn primarily from Generation Z (born circa 1997–2012) and soon from Generation Alpha (born 2013 onward, once over 18), embody not only different age cohorts but also profoundly distinct worldviews shaped by digital saturation, economic uncertainty, and evolving social norms.

At the same time, military leadership must now navigate an increasingly polarised and disoriented information landscape often referred to as the 'post-truth era'. The term "post-truth" was popularised by author Ralph Keyes in his 2004 work *The Post-Truth Era*² and later gained widespread recognition when Oxford Dictionaries selected it as their 2016 'Word of the Year'. In this environment, facts are often drowned out by emotional noise, many of which are propagated through the same online spaces younger soldiers live in. In such a context, leadership is no longer solely about commanding respect; it requires earning trust within a contested information space. The academic literature on post-truth challenges has revealed the emergence of several contrasting themes.³

This generational and informational shift poses a direct challenge to traditional command structures. As new recruits arrive with different expectations of authority, communication, and values, the DF must reconsider how it develops, deploys, and sustains leadership at all ranks. This paper argues that the solution lies not in abandoning tradition but in adapting it with emotional intelligence, mission clarity, and digital fluency. This paper explores how leadership in the DF must evolve to meet the demands of the current and future era, drawing on both established doctrine and emerging best practice to build resilient, engaged, and ethically grounded future leaders.

It will do this by first analysing the defining characteristics of Gen Z and Gen Alpha, exploring how these influence their perceptions of authority, communication preferences, and expectations of leadership. It will then examine the challenges of the post-truth era and hybrid threat environment, assessing their impact on leadership credibility and operational cohesion. Following this, the paper will discuss evolving leadership approaches, including relational and adaptive models, with insights from both contemporary scholarship and practical military experience. Finally, it will consider strategies for fostering inter-generational cohesion within the DF and present conclusions on how leadership can be most effectively adapted to meet the demands of a rapidly changing strategic and societal landscape.

¹ Government of Ireland. *Defence Policy Review 2024: Adjusting and Affirming Our Defence Policy in an Era of Change* (Dublin: Department of Defence, 2024), 5.

² Ralph Keyes, *The Post-Truth Era: Dishonesty and Deception in Contemporary Life* (New York: St. Martin's Press, 2004), 16.

³ Lee McIntyre, *Post-Truth* (Cambridge: MIT Press, 2018), 13.

Generational Profiles: Who Are Gen Z and Gen Alpha?

Gen Z is the first cohort raised entirely within the digital age. They are defined by high digital fluency, a preference for visual and instantaneous communication, and a strong desire for transparency, purpose, and ethical integrity in their professional environments.⁴

Gen Alpha, now entering adolescence, is expected to intensify these characteristics. This cohort is growing up in an environment shaped by artificial intelligence, gamification, and constant connectivity, blending virtual and physical experiences in their worldviews. More recent attention in the literature has focused on the provision of digital education and literacy in shaping their identities.⁵

Both generations are most responsive to leadership that is authentic, empathetic, and consistent traits that sometimes diverge from traditional hierarchical military models. Much of the current literature on Gen Z leadership expectations pays particular attention to purpose-driven work and value alignment.⁶ A 2022 survey by Deloitte showed that in a Global Gen Z and Millennial Survey, mental health, purpose, and inclusion now rank among the top workplace priorities for young professionals, often above salary or promotion prospects. This shift is increasingly reflected in DF recruit feedback and exit interview data.⁷

For many, purpose-driven work means contributing to missions that have a clear and positive social impact. In the context of the DF, this often aligns with the organisation's long history of deploying soldiers on peace support and crisis management operations. Deployments with the United Nations, for example, not only demonstrate Ireland's values-based culture of service, neutrality, and respect for human dignity but also provide younger personnel with a tangible connection between their daily duties and the broader influence on world peace they might help achieve.

Within military contexts, these traits require leaders to reframe how they build authority and inspire loyalty. Gens Z and Alpha do not reject structure; they expect structure that makes sense, leadership that listens, and missions that matter. The DF Leadership Doctrine supports this generational expectation by explicitly stating that "people-centred leadership" is a core value, emphasising respect, moral courage, and development of subordinates as pillars of command.⁸

4 Jean Marie Twenge, *iGen: Why Today's Super-Connected Kids Are Growing Up Less Rebellious, More Tolerant, Less Happy—and Completely Unprepared for Adulthood* (New York: Atria Books, 2017), 48.

5 Mark McCrindle and Ashley Fell, *Generation Alpha: Understanding Our Children and Helping Them Thrive* (Sydney: Hachette Australia, 2021), 18.

6 Corey Seemiller and Meghan Grace, *Generation Z Leads: A Guide for Developing the Leadership Capacity of Generation Z Students* (North Charleston, SC: CreateSpace, 2018), 23.

7 Michele Parmelee, "Don't want to lose your Gen Z and millennial talent? Here's what you can do," *Deloitte Insights*, (2022), <https://www.deloitte.com/us/en/insights/topics/talent/deloitte-millennial-survey.html>

8 Irish Defence Forces, *Leadership Doctrine*. (Dublin: Defence Forces Printing Press, 2016.), 16.

The Post-Truth World: Threats to Authority and Cohesion

The post-truth era refers to circumstances where emotional resonance overrides factual accuracy in shaping belief and action. This presents real leadership difficulties that extend far beyond orders and procedures. Trust in institutions is waning, misinformation is rising, and shared realities are fragmenting, all of which affect how young personnel perceive authority, interpret discipline, and relate to group cohesion. Previous research findings into military trust dynamics in the digital age have been inconsistent and contradictory.⁹ In Ireland, this is particularly pertinent. Political discourse and digital platforms have facilitated the spread of anti-establishment narratives, some of which explicitly target the DF.¹⁰

An article by the European Security Journal cautions that such dynamics can degrade unit cohesion, especially for younger service members who are constantly exposed to competing, often manipulative, digital narratives. A large and growing body of literature has investigated the cognitive and emotional impact of misinformation on military cohesion.¹¹ The DF Leadership Doctrine warns against complacency in maintaining moral authority, reinforcing that “leaders must uphold the highest standards of integrity and model behaviours expected of their subordinates.”¹² This is particularly relevant when trust and truth are contested terrain.

The Erosion of Authority and the Rise of Peer Credibility

Traditional models of military authority rely on hierarchy, command structures, and institutional credibility. However, for these generations, trust is increasingly decentralised. Young personnel are more likely to validate leadership messages through peer consensus, online communities, or lived authenticity than through position or rank alone. This presents a subtle but serious leadership challenge within the DF.

In the post-truth era, where misinformation thrives and institutions are routinely questioned, credibility must be earned, not assumed. A DF junior leader’s message shared informally through WhatsApp may hold more influence than an official policy brief if the former feels more relatable, transparent, or aligned with shared values. As noted in research on digital-era military psychology, “authority that does not align with perceived authenticity is quickly bypassed or resisted.”¹³ This does not imply a rejection of structure. Rather, it signals the importance of authentic presence, two-way communication, and visible competence. Leaders must not only speak clearly but also demonstrate relevance, whether in a field exercise, values discussion, or online forum. The DF Leadership Doctrine affirms that leadership must “model ethical behaviour and exercise influence through trust and respect,” principles that are increasingly critical as peer credibility rivals command authority.¹⁴

9 Roger C. Mayer, James H. Davis, and F. David Schoorman. “An Integrative Model of Organizational Trust,” *Academy of Management Review* 20, no. 3 (1995), 715.

10 Eunan O’Halpin, “Ireland and Disinformation: National Security in the Digital Age,” *Irish Studies in International Affairs* 32, no. 1 (2021), 82.

11 European Security Journal. “Misinformation, Disinformation, and the Threat to Military Cohesion,” *European Security Journal*, (2020), 3.

12 Defence Forces, *Leadership Doctrine*, 27.

13 Uzi Ben-Shalom, Zeev Lehrer, and Eyal Ben-Ari, “Cohesion during Military Operations: A Field Study on Combat Units in the Al-Aqsa Intifada,” *Armed Forces & Society* 32, no. 1 (2005): 70.

14 Defence Forces, *Leadership Doctrine*, 35.

By acknowledging and adapting to these shifts in influence, DF leaders can strengthen cohesion without diluting standards. Building horizontal trust (among peers) and vertical trust (within the chain of command) must be seen not as separate goals, but as mutually reinforcing. When institutional leadership complements rather than competes with peer validation, younger soldiers are more likely to align with mission objectives and internalise organisational values.

Adaptive and Blended Leadership Models

It is worth exploring some of the more pertinent leadership models to see which could be most effective in engaging Gen Z and Gen Alpha. The DF has historically leaned on transactional leadership rooted in authority, compliance, and procedural fidelity. While effective in certain operational contexts, this model alone is insufficient for leading Gen Z and Gen Alpha, who place a high value on rationale, purpose, and relational clarity in how they are led. The DF Leadership Doctrine acknowledges that “the challenge for modern leaders is to adapt to changing environments while maintaining the mission focus and values of the organisation.”¹⁵ This need for adaptation is not unique to Ireland; research across Western militaries shows a growing shift toward leadership models that blend transactional efficiency with transformational, ethical, and authentic leadership approaches.¹⁶ Transformational leadership theory, first articulated by James MacGregor Burns in the late 1970s, has gained significant traction within military organisations due to its focus on inspiring, motivating, and developing subordinates through shared purpose and vision.¹⁷ Ethical and authentic leadership further strengthen this approach by ensuring that decision-making and leader behaviour are grounded in transparency, moral integrity, and consistency, all qualities that align strongly with the expectations of Gen Z and Gen Alpha, who demand leaders they can trust both personally and professionally. For digitally native, socially conscious recruits, the combination of transformational inspiration, ethical grounding, and authentic engagement is far more compelling than authority alone.

The DF Leadership Doctrine acknowledges that “the challenge for modern leaders is to adapt to changing environments while maintaining the mission focus and values of the organisation.”¹⁸ This doctrinal emphasis on flexibility, empathy, and mission command reinforces the need for blended leadership approaches in today’s evolving military landscape particularly when engaging digitally native, socially conscious generations. Heifetz and Linsky’s theory of adaptive leadership urges leaders to navigate complex systems by adjusting their style and diagnosing the political and psychological dynamics at play. The existing literature on adaptive leadership is extensive and focuses particularly on complex social systems.¹⁹ These perspectives are discussed here because they, along with related bodies of work on transformational, ethical, and authentic leadership, provide complementary frameworks for understanding how the DF can engage and inspire younger generations in an era of rapid social, technological, and strategic change.

¹⁵ Defence Forces, *Leadership Doctrine*, 11.

¹⁶ Leonard Wong, Paul Bliese, and Thomas James Halverson, *Developing Adaptive Leaders: The Crucible Experience of Operation Iraqi Freedom* (Carlisle: Strategic Studies Institute, U.S. Army War College, 2003), 25.

¹⁷ James MacGregor Burns, *Leadership*. (New York: Harper & Row, 1978), 20.

¹⁸ Defence Forces, *Leadership Doctrine*, 11.

¹⁹ Ronald A. Heifetz, and Marty Linsky, *Leadership on the Line: Staying Alive through the Dangers of Leading* (Boston, MA: Harvard Business Review Press, 2002), 32.

Blended leadership, which combines transformational methods (inspiring through shared vision) and servant leadership (prioritising the well-being and development of subordinates), is especially resonant with younger generations. These models emphasise purpose, personal integrity, and mentorship attributes that consistently show are vital to Gen Z engagement. Simon Sinek's *Leaders Eat Last* illustrates how trust, empathy, and social connection within leadership relationships drive performance, loyalty, and cohesion in high-pressure environments.²⁰

In the DF context, these three leadership approaches intersect in meaningful ways. Adaptive leadership provides the framework for navigating uncertainty by encouraging leaders to continually assess their environment, adjust their style, and address both operational challenges and the underlying human dynamics that influence unit performance. Transformational and servant leadership complement this by focusing on shared purpose, moral integrity, and the development of subordinates, creating leaders who inspire through vision while prioritising the well-being of their people. Finally, Sinek's trust-based leadership principles highlight the importance of building psychological safety and mutual loyalty, particularly in high-stress operational contexts. Together, these approaches offer a blended model that addresses the strategic, relational, and moral dimensions of command. Within the DF, such an integrated style allows leaders to maintain the discipline and mission focus essential to military effectiveness while remaining relevant to digitally native, socially conscious generations. In an era defined by cognitive warfare and post-truth narratives, the ability to combine adaptability, inspiration, and trust is no longer optional; it is a core competency for sustaining cohesion and operational effectiveness.

The Link to Hybrid Warfare and Cognitive Resilience

Hybrid warfare, which combines conventional forces with cyber tactics, disinformation, and psychological manipulation, targets morale and cohesion as much as infrastructure. For example, during the 2014 Crimea annexation, coordinated military operations were accompanied by cyberattacks on infrastructure and widespread disinformation campaigns aimed at undermining public trust. The literature on cognitive warfare has highlighted several strategic frameworks for resilience development.²¹ Their exposure to online content makes younger personnel especially susceptible to manipulation, but with proper leadership, they become key actors in building cognitive resilience. Empowered, engaged, and ethically grounded junior personnel are the first line of defence against both misinformation and internal demoralisation.²² The DF Leadership Doctrine points to "moral courage" being essential to operational readiness, especially in situations where personnel must critically assess information, resist manipulation, and act with integrity in ambiguous environments.²³ This attribute is particularly relevant in the evolving information battlespace, where psychological and cognitive threats can erode trust and cohesion as effectively as physical attacks.

NATO's 2022 Cyber Awareness Report urges investment in "cognitive security," embedding trust, critical thinking, and digital literacy within defence culture. This

20 Simon Sinek, *Leaders Eat Last: Why Some Teams Pull Together and Others Don't* (New York: Portfolio/Penguin, 2014), 45.

21 NATO, *Countering Cognitive Warfare: NATO's Approach to Resilience* (Brussels: NATO Defence College, 2021), 12.

22 Jon R. Lindsay and Erik Gartzke, "Cognitive Security and Military Effectiveness in the Digital Age," *Journal of Strategic Studies* 44, no. 3 (2021): 430.

23 Defence Forces, *Leadership Doctrine*, 19.

requires developing leaders who can safeguard the mental resilience of their units, not merely acquiring better technology.²⁴ For the DF, this lesson is clear. Cognitive resilience must be treated as a leadership priority, both in joint task force planning and in the daily life of every unit. This includes structured digital education, open discussions about disinformation, and fostering a command climate where personnel feel confident reporting suspicious narratives without fear of reprisal. Hybrid warfare is no longer confined to cyberattacks or the deployment of drones it is also fought over narratives, trust, and perception. Leaders in this environment must serve not only as tactical decision-makers but also as cognitive anchors, ensuring that their personnel are prepared for both the visible battles on the ground and the invisible battles for the mind.

Practical Leadership Techniques for the DF Context

Based on a thorough review of the literature on the topics discussed above, I propose four practical leadership techniques. Firstly, transparent communication, being honest about institutional challenges and avoiding vague or ambiguous directives help young soldiers connect with the mission and see where they fit in. There is a large volume of published studies describing the role of communication in strengthening leader credibility and organisational trust.²⁵

Secondly, I argue that structured empathy, practised within a disciplined framework, enhances both performance and cohesion. Demonstrating genuine interest in individual motivations while upholding standards can create a leadership presence that is both respected and followed. For example, a DF junior leader who takes the time to understand a soldier's long-term career goals, while pushing them to excel, can foster loyalty and higher performance, as the soldier sees that personal development and mission standards are aligned.

Thirdly, mission command with constraints, delegating responsibility within clear operational parameters, builds adaptive judgment in junior personnel, enabling them to function independently when needed. A considerable amount of literature has been published on distributed command structures and their effect on junior leader adaptability. For example, during NATO's Enhanced Forward Presence in the Baltic States, battlegroups reported that clearly defined mission intent, paired with freedom to adjust tactics in the field, improved decision-making speed and operational flexibility among junior leaders.²⁶

Finally, mentorship, both formal and informal, bridges generational gaps and accelerates leader development. Cross-rank mentorship also fosters deeper respect between junior and senior personnel.

In one example from Air Corps (AC) Base Security, a Gen Z airman was given responsibility for drafting a social media policy to provide a better understanding for camp staff during a high-profile prisoner extradition. The product was both functional and innovative, but more importantly, it demonstrated to the airman and his peers that their input was

²⁴ NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Defence Awareness Report 2022*. (Tallinn: NATO CCDCOE, 2022), 7.

²⁵ Linjuan Rita Men, and Bruce Kent. Berger. "Leadership, Communication, and Trust: Exploring the Impact of Transparent Communication on Employee Organization Relationships." *Public Relations Review* 45, no. 5 (2019): Article 101781.

²⁶ Boas Shamir and Eyal Ben-Ari. "Military Mission Command: The Who, What, Where, When, and Why Not." *Armed Forces & Society* 27, no. 1 (2000): 61.

valued and impactful. During a recent career course to train selected AC personnel to become junior leaders, implementing weekly one-to-one debriefs on their performance transformed morale. Students did not undermine authority but respected it more when their insights were acknowledged and, where appropriate, acted upon. This was adaptive leadership in action.

The DF Leadership Doctrine explicitly encourages leaders to develop their subordinates through trust, opportunity, and values-based mentoring.²⁷ For example, during joint public order training, junior leaders were assigned as liaison observers, a role also given to senior NCOs. The result was a noticeable improvement in engagement and awareness, and participants reported increased confidence and purpose. Leadership techniques must therefore be taught and reinforced through experiential learning, not just classroom theory. Leader development courses, such as junior leadership training, should be reviewed to ensure they include scenario-based exercises that simulate generational communication challenges, decision-making under digital ambiguity, and mission execution under high autonomy. This embeds not only tactical competence but also cognitive and emotional fluency key traits for leading Gen Z and Alpha.

Challenges and Risks

Naturally, there are challenges and risks to the suggestions I have outlined above. For example, over-accommodating generational preferences risks eroding military discipline. While modern leadership must engage Gen Z and Gen Alpha on their terms, the core standards of integrity, courage, and accountability cannot be compromised. The generalisability of much published research on generational leadership in high-stakes environments remains problematic.²⁸

A secondary risk is generational misalignment within leadership hierarchies. Senior leaders raised in different eras may misinterpret Gen Z communication norms as insolence or fragility. Conversely, younger soldiers may mistake stoicism for apathy. Mutual education and empathy are key to resolving this tension. A hypothetical example of this tension could arise during a debrief in a DF unit, where a junior soldier's use of emojis or slang in a written communication could be viewed as unprofessional by a senior leader. The intent is positive, but the format undermined credibility in the eyes of the chain of command. Such generational misreads can quickly erode morale or, worse, provoke disciplinary friction.

To bridge this gap, the DF should consider integrating digital communication literacy into leader development. Senior leaders must learn to decode emerging communication styles without dismissing their intent, while younger members should be trained in correct military writing, communication formality, and appropriateness of tone and content. The DF Leadership Doctrine acknowledges that “the human dimension of leadership requires mutual understanding across ranks and contexts.”²⁹ Institutionalising intergenerational awareness as a leadership competency will help future-proof cohesion.

²⁷ Defence Forces, *Leadership Doctrine*, 38.

²⁸ Jennifer J. Deal, David G. Altman, and Steven G. Rogelberg, “Millennials at Work: What We Know and What We Need to Do (If Anything),” *Journal of Business and Psychology* 25, no. 2 (2010): 193.

²⁹ Defence Forces, *Leadership Doctrine*, 44.

Finally, leaders must avoid confusing emotional intelligence with passivity. Empathy must be balanced with decisiveness, and tolerance must not substitute for clarity. Hybrid warfare is fought with confident, communicative, and culturally competent leaders, not with those who capitulate to ambiguity. The doctrine reinforces this balance by stating that “leadership must be morally courageous, clear in purpose, and decisive in application, even in uncertainty.”³⁰

Conclusion: Leading into the Cognitive Era

The nature of leadership in the DF is changing, not because tradition has failed, but because the operating environment and those who serve within it have evolved. Gen Z and Gen Alpha bring with them distinct expectations of transparency, relevance, and ethical integrity. In an age shaped by digital saturation, polarised narratives, and hybrid threats, military leaders must be more than authoritative; they must be authentic, adaptable, and trusted.

From my perspective, the post-truth era has demonstrated that influence can no longer rely on rank alone. The leaders I have observed and those I have served under who have succeeded in this environment are those who communicate clearly, live the values they espouse, and invest time in building trust both vertically and horizontally. The DF Leadership Doctrine provides the foundation for this, but it is up to us, as current and future leaders, to translate it into action in a way that is relevant to the generations we now lead. In hybrid warfare scenarios, I have seen how trust and cognitive resilience can be the difference between maintaining operational tempo and experiencing breakdowns in decision-making. Leaders who take the time to understand their people, align them with mission purpose, and equip them with critical thinking skills are far better positioned to navigate the uncertainty and complexity of modern operations.

As we transform, the future DF will not be defined solely by equipment or tactics, but by the calibre of its people and the culture that shapes them. This means meeting new generations where they are listening to their perspectives, aligning them with the DF core mission, and giving them the tools to meet, even exceed our standards; and also to foster a force that is both operationally effective and morally grounded. For me, this is the essence of leading into the cognitive era: a commitment to blending tradition with innovation, holding fast to the timeless values of service, integrity, and excellence, while adapting our leadership to remain relevant, credible, and trusted in an era of rapid change.

The objective is not to lower standards, but to elevate and support individuals in reaching the standards that have long been set.

³⁰ Defence Forces, *Leadership Doctrine*, 52.



The Return of (Maritime) Hybrid Warfare as a Leadership Challenge for Europe's Democracies

Dr Brendan Flynn

A Wake-up Call Ignored?

Long before any full-scale invasion, in late 2018, three small Ukrainian naval vessels were rammed, shot up and seized while attempting innocent passage into the Kerch Strait-Azov Sea.¹ The result was an immediate crisis that threatened the complete breakdown of a shaky ceasefire. Ukraine called for NATO warships to enter the Black Sea to affirm their rights under international law, while the Russian side countered with a barrage of disinformation which challenged the legality of the Ukrainian actions.² Many Western leaders, notably Germany's Angela Merkel, rushed to urge restraint, the latter adding that there could be "no military solution."³

This paper explores leadership in crises like this, drawing attention to shock, surprise, and decision-maker overload. While these phenomena have been well discussed as a military leadership problem at the tactical level,⁴ they also operate at the operational and strategic levels and extend to civilian leaders.⁵ Yet much of the literature describes leadership shock under war conditions or nuclear risks, whereas in hybrid scenarios, violence is often initially denied or minimized but nonetheless present. Paradoxically under a peace-time mindset, shock and surprise may have greater effect.⁶ Like many other hybrid attacks, the Kerch Strait crisis produced short-term (24-72hr) shock and paralysis among key Western decision-makers.⁷ The immediate 'restraint' narrative, while seemingly sensible, unquestionably gave the initiative to Russian forces. Moreover, the outcome offered the perverse lesson for Putin that Western countries would not support Ukraine in a fight.

In retrospect, this now obscure crisis was a textbook example of hybrid operations at sea and a wake-up call ignored. It also showed how Western leadership had learned little from the events of Crimea in 2014. They easily allowed themselves to be surprised and failed to coordinate with Ukrainian leaders. Today, novel hybrid maritime scenarios are emerging. Have Western decision-makers developed a leadership style to appropriately respond?

This paper proceeds by first exploring some general misconceptions about hybrid threats and explains how today's hybrid activities have moved to sea. A diverse spectrum of maritime hybrid threats is stressed, and how this range poses challenges for leaders who must respond to everything from merely aggressive signalling behaviour at sea, to high stakes violent confrontations. The final sections consider how leadership can be made more resilient and how it differs across the tactical, operational, and strategic levels.

1 Under international law, these remain Ukrainian territorial waters, as Russian annexation is not recognized by an overwhelming majority of states in the UN system and indeed was condemned by a specific Resolution of the General Assembly, No 68/262, 1/04/2014.

2 Patrick Wintour, "Ukraine President Calls for NATO Warships in Sea of Azov," *The Guardian*, November 29, 2018, <https://www.theguardian.com/world/2018/nov/29/russia-blocked-ukrainian-azov-sea-ports-minister>

3 Restraint was specifically urged by UN Secretary-General António Guterres, NATO, and the EU. For an example of the tone of the German response, see: Deutsch Welle, "Merkel urges Putin to release Ukraine sailors," November 12, 2018, <https://www.dw.com/en/angela-merkel-urges-vladimir-putin-to-release-ukrainian-sailors/a-46672124>

4 For specific discussions of shock as a tactical leadership challenge, see B.A. Friedman, *On tactics: A Theory of Victory in Battle* (Annapolis: Naval Institute Press, 2017), chap 10 and Jim Storr, *The Human Face of War* (London: A&C Black, 2009), chap 5.

5 For a general and rounded discussion of how surprise delivers shock to senior civilian and military leaders see Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Georgetown University Press, 2013) and Mark F. Cancian, *Coping with Surprise in Great Power Conflicts* (New York: Bloomsbury, 2018). For a succinct overview of the ambiguous value of surprise attacks in modern warfare see Lawrence Freedman, "Beyond Surprise Attack," *Parameters* 47, no. 2 (2017).

6 For a somewhat inconclusive discussion see Andrew Dolan, "Hybrid Warfare and Strategic Surprise," in *Hybrid Warfare Reference Curriculum Volume III Elective Lectures*, ed. Jobbágy Zoltán and Edina Zsigmond (Ludovika University Press, 2025), 161-176.

7 For background to the incident, see Jonathan Stevenson (ed.)/IISS, "The Kerch Strait incident," *Strategic Comments* 24, no. 10, (2018): i-ii.

(Mis)Understanding Evolving Hybrid Threats

After Russia's illegal annexation of Crimea in 2014, the widely misunderstood "little green men" narrative emerged. A few commentators assumed that hybrid threats are mostly low-risk or involve little or no violence.⁸ In fact, hybrid operations often feature significant violence towards property, institutions and people, even if such can be initially downplayed. The Ukrainian sailors at the Kerch Strait were lucky to escape with their lives and were illegally held captive for over 10 months. Moreover, we should not forget that the mythic "little green men" narrative of 2014 masked what was a violently executed territorial invasion.

Since then, hybrid threats have not disappeared or become less of a challenge, but partly moved to sea. Indeed, parallel with the open warfare in Ukraine, a shadowy, covert, and hybrid confrontation has emerged across Europe and beyond.⁹ In September 2022, with the war raging in Ukraine, the Nordstream pipeline was spectacularly sabotaged. This generated intense speculation that successively favoured different 'who done it' theories: either an improvised Ukrainian covert operation, American special operations forces, or Russian vessels. Regardless of provenance, the sabotage of Nordstream has transformed awareness of maritime hybrid threats: they are no longer hypothetical. It has also awakened a sensitivity towards critical maritime infrastructure, where before there was a rather typical 'sea blindness'.

The face of Maritime Hybrid Warfare?

In the Baltic Sea there have been heightened tensions over the possibility of deliberate sabotage of sub-sea cables. A series of events occurred close together over 2023-2025 which seem statistically improbable, although it is worth noting that many subsea cable industry experts have stressed that accidental damage to cables is commonplace. Moreover, there is a very high level of technical redundancy in such systems. The internet is not so easily switched off and repair times can be surprisingly fast-sometimes weeks.

⁸ On this point see: Alina Bărgăoanu and Elena Negrea-Busuioacă, "Hybrid Warfare is Less Than Warfare: A Dangerous Illusion," *IW Perspectives*, (July 21, 2024), https://irregularwarfarecenter.org/wp-content/uploads/P_19_Hybrid_Warfare_is_Less_Than_Warfare.pdf

⁹ For an overview in the public domain, see "Russian sabotage attacks surged across Europe in 2024: This year's apparent lull may be the calm before another storm," *The Economist*, (July 22, 2025). See also Caspar Hobhouse, On A War Footing: Securing critical energy infrastructure, Brief 21, August (EISS, 2025), https://www.iss.europa.eu/sites/default/files/2025-08/Brief_2025-21_Energy%20security.pdf



https://en.wikipedia.org/wiki/Kashtan-class_salvage_vessel#/media/File:June_2020_Baltic_Fleet_submarine_rescue_exercise_-_Kashtan-class_SS-750_launching_AS-26_DSRV.jpg

A Russian Kashtan class auxiliary vessel, named SS-750, of a type that could be used for maritime sabotage operations. This exact vessel was proximate to the Nordstream explosions before the key dates of 26-27th September 2022 when the pipeline was blown up by explosives. Obviously, this is not proof of any wrongdoing or responsibility.

However, much greater losses would arise if sub-sea gas and electricity connector pipelines are sabotaged. On Christmas Day 2024 the Eagle S merchant ship was detained by Finnish Border Guards after dragging its anchor and severing an electricity cable, which are expensive and slow to replace. Losses to grid stability and energy supply from gas pipelines and electricity cable cuts are more strategically significant given that European countries have reduced (but not actually ended) their dependence on Russian oil and gas exports.

Indeed, some types of vulnerability have merely been swapped for another. The much greater reliance on American and Qatari sourced LNG for example, is increasingly stored in large and vulnerable FSRUs (Floating Storage Regasification Units). Ireland has plans for a single example to be berthed near Tarbet adding considerably to our energy security of supply.¹⁰ We are a latecomer here, as Germany, Netherlands, Finland and Lithuania have several contracted in the wake of the Ukraine invasion.

¹⁰ See: "Strategic Gas Emergency Reserve", accessed Sept. 16 2025, <https://www.gasnetworks.ie/about/projects/strategic-gas-emergency-reserve>



Image: https://commons.wikimedia.org/wiki/File:FSRU_Independence_in_the_port_of_Klaip%C4%97da_Lithuania.jpg

Sitting Duck? Since 2014 Lithuania has contracted for an FSRU, called Independence, docked at their port of Klaipėda, to reduce its reliance on Russian gas supplies. In 2022 they became the first European country to completely cut themselves off from Russian gas imports.

Why and How Conduct Hybrid Operations at Sea?

Unfortunately, such ships could be easily targeted. A hybrid attack on these assets may seem implausible to us, but could be rationalised as crude signalling. Removing and evading existing sanctions or deterring/punishing any new measures remains a clear Russian priority. Hybrid scenarios at sea here offer a readily available “horizontal escalation” opportunity, whereby one geopolitical rival seeks to deter or coerce others by imposing costs in a different space/place from their main site of conflict.¹¹ This can also involve a different type of threat, employing economic warfare, propaganda, use of proxy forces or today, cyber hacking. Moving conflict from land to sea fits this logic.

We should also be mindful that hybrid threats at sea do not always require specialist divers or expensive James Bond technologies. A basic Mavic-style drone costs approximately \$5,000 USD.¹² A significant swarm attack with 50 units can be funded for as little as a quarter of a million dollars. A single FSRU costs at least over one hundred million dollars and is not easily replaceable. Even a limited attack could create crippling costs through marine insurance markets, which are very sensitive to war risks.

Less widely known is the phenomenon of jamming or spoofing of GPS and Automatic

¹¹ Martin C. Libicki, *The New Calculus of Escalation: Avoiding Armageddon in Great Power Conflict* (Washington, D.C.: Georgetown University Press, 2025), 5. See also for a wider discussion of possible Russian escalation pathways: Bryan Frederick, Mark Cozad, and Alexandra Stark, *Escalation in the War in Ukraine: Lessons Learned and Risks for the Future* (RAND, 2023), 17-20.

¹² See: David Hambling, “Moving Targets: Implications of the Russo-Ukrainian War for Drone Terrorism,” *CTC Sentinel* 18, no.7 (2025), <https://ctc.westpoint.edu/moving-targets-implications-of-the-russo-ukrainian-war-for-drone-terrorism/>

Identification System (AIS)¹³ navigational systems in the Baltic and the Black Sea. These signals are heavily relied upon by civil and military maritime and air traffic. As of mid-2025, the practice of GPS jamming has not spread to the wider Atlantic, although there are signs that Russian jamming capabilities have moved from land-based emitters to mobile ship-based systems, which means the threat can move well beyond the Baltic.¹⁴

Also receiving less media attention, is an enormous Russian merchant shipping effort which operates “hiding in the plain sight.” This “shadow fleet” of oil tankers subverts sanctions and allows Russia’s war machine to recapitalize. These vessels are often improperly registered with flags of convenience, and the seaworthiness of the vessels is a concern. Often old they frequently have opaque insurance arrangements, and should raise alarm bells for a potential ecological catastrophe. Equally, if these ‘shadow vessels’ are detained, this could provide a flashpoint. As of mid-2025, Russian Navy warships have begun occasional “escorts” of such vessels, which poses obvious scope for an armed incident. It is worth observing that a significant number (>200+) of such vessels have been documented transiting through Ireland’s EEZ in the first half of 2025,¹⁵ which poses a significant challenge for Ireland’s relatively austere maritime presence and monitoring capabilities.

Understanding the Maritime Hybrid Threat Spectrum

Figure 1 below illustrates a ‘thermometer’ conception of maritime hybrid threats which shows that while the threat of violence is only present at the higher end, it is nonetheless far from trivial. Moreover, the whole purpose of a ‘thermometer conception’ of threats is to understand that scenarios can evolve fast, veering from low-risk operations to those where violence is quite possible.

Also of note is the legal complexity inherent in many of these scenarios. Where a suspicious vessel has been identified sailing within international waters, the general powers to stop, search and arrest a vessel are limited. Territorial waters typically extend to 12 nautical miles (20.1 km). Exclusive Economic Zones, although much further in extent, do not confer strong jurisdictional policing powers but instead authority for permitting energy, extractive industry or fishing activities.

13 For details on GPS and AIS in marine navigation, see: “How Do GPS Systems Aid Maritime Navigation?”, accessed Sept.16th 2025, <https://maersktraining.com/news-and-insights/industry-insights-blog/how-do-gps-systems-aid-maritime-navigation> and “AIS (Automatic Identification System) overview”, accessed Sept.16th 2025, <https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview>

14 See MI News Network, “Moving Ships Likely Behind GPS Jamming In Baltic Sea, Study Finds,” *Shipping News*, March 4, 2025, <https://www.marineinsight.com/shipping-news/moving-ships-likely-behind-gps-jamming-in-baltic-sea-study-finds/>

15 Jackie Fox, “Data flags hundreds of Russian ‘shadow fleet’ visits to Irish EEZ,” *RTE News*, July 25, 2025, <https://www.rte.ie/news/prime-time/2025/0724/1525050-shadow-fleet-irish-eez/>

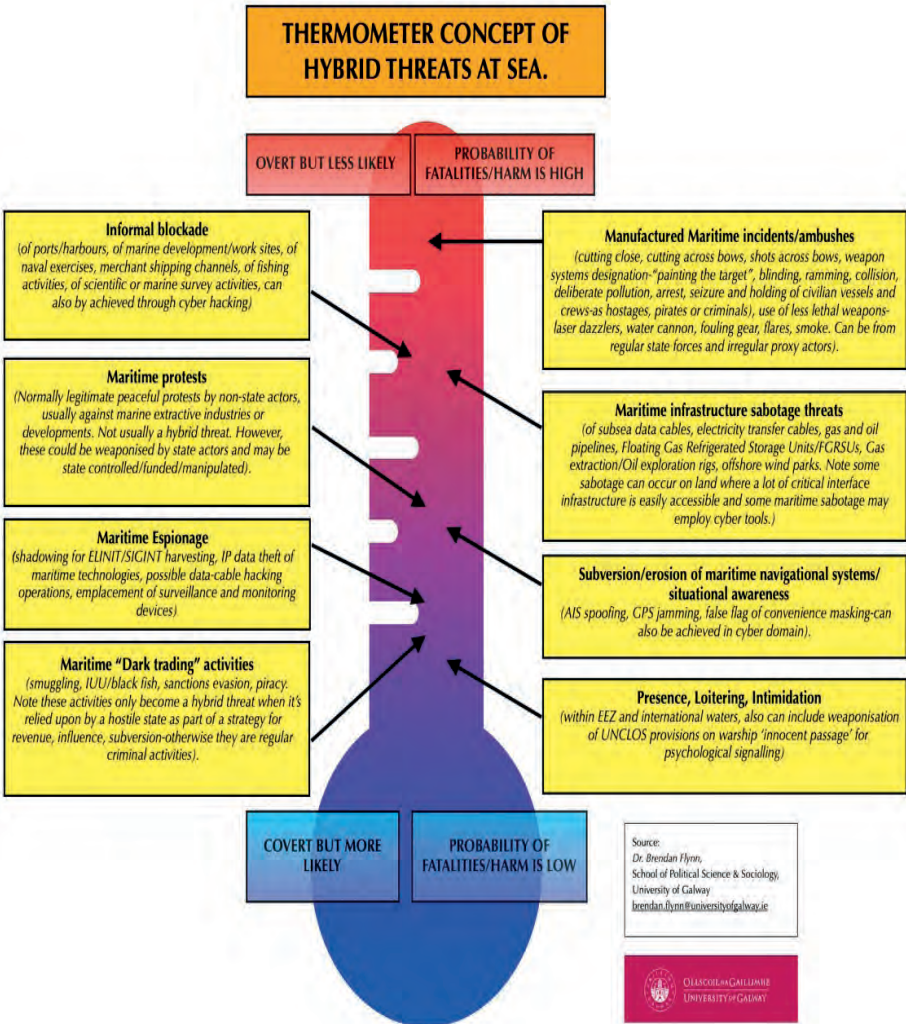


Figure 1: Thermometer Concept

In the Kerch Strait incident, both sides made competing legal claims. Making a determination of the legalities of the situation can take time, and that gives an advantage to the hybrid aggressor. It allows 'fake news' and disinformation narratives to amplify. However, leaders can mitigate this risk by having maritime legal expertise readily available and by rehearsing scenarios in war-gaming or simulation exercises. Such legal expertise often exists in-house, provided by naval or other state lawyers, but also important are authoritative, impartial legal experts, and increasingly OSINT social media activists, whose 'quick takes' need to be either refuted or acknowledged with speed. There certainly needs to be dissemination that is social media savvy to establish the legal rights and wrongs for an information cycle that now runs in hours rather than days.

Shock-Proofing Leadership for Maritime Hybrid Crises

The most immediate leadership challenge in a hybrid crisis is to co-ordinate and delegate effectively in a situation that will usually evolve quickly and under conditions of uncertainty. The literature on dynamic decision-making in crises and the need for training in this area is here instructive.¹⁶ Close and timely coordination between civil and military authorities is essential, but perhaps more challenging is that between private commercial firms and public bodies. This coordination challenge is often severely underestimated and typically only revealed through repeated exercises and simulations.¹⁷ To be effective, these need to include not just civil and military agencies or their specialists, but also senior civilian leaders.

While most Western civilian leaders understand the broad idea of hybrid threats, there may still be confusion over whether significant violence will feature. Therefore, a comforting assumption can take hold that any crisis will be mainly an intelligence, police or cybersecurity matter. As has been stressed here, this is mistaken because significant violence is often a feature. Moreover, military assets such as specialist aircraft, vessels or vehicles will typically be required as an aid to the civil powers. Nonetheless, the threshold of provocation is likely to remain well below that of recognised hostilities, so military assistance must be appropriate. Leadership here is then about discrimination and responding carefully with public messaging. Civil and military leaders need to show resolve, but not overplay the hybrid threat either.

Unfortunately, a common weakness of Western leadership in hybrid crises is a fear of escalation when faced with violence. The sensible goal in almost every case is certainly not to escalate. Nobody wants a shooting incident to become a shooting war. Yet this rationale does not mean de-escalation is warranted in every case. Indeed, if hostile actors perceive a retreat or a complete unwillingness to use force, they may be emboldened.¹⁸ The Ukrainian flotilla at Kerch was attacked precisely as it was retreating home.

Presence in the form of naval ship patrols, drones, sensors, and significant supporting assets, such as patrol aircraft or fast jets, will likely achieve a deterrent effect, provided it is appropriate to the threat; otherwise, it can be weaponised by an adversary and portrayed as escalatory. To be truly effective, presence in the maritime space requires a blend of continuity and surge capabilities, so adversaries understand that they are being routinely monitored but can also face very rapid, reinforced responses should they pose a threat.

A mix of clear red lines together with some degree of uncertainty and unpredictability seems to offer the best chance of deterring any adversary from escalation.¹⁹ However, one must be cautious not to fall into the trap of assuming perfect rationality or that adversaries

16 On dynamic decision making see Bjørn T. Bakken, Thorvald Hærem and Inger Lund-Kordahl, "Building Competence Against Hybrid Threats Training and exercising hybrid command organizations," 234-250 in Odd Jarl Borch and Tormod Heier (Eds.), *Preparing For Hybrid Threats To Security Collaborative Preparedness and Response* (Routledge, 2025).

17 For examples of these and insight about the scale of the co-ordination challenge see, Paul Ames (et al.), *Leaders' response to hybrid threats: a real-time case study*, (Friends of Europe, 2019) https://www.friendsofeurope.org/wp/wp-content/uploads/2019/07/FoE_Leaders-response-to-hybrid-threats_2019.pdf and Hedlund, Erik and Aida Alvinus, "Team Learning in Civil–Military Collaboration Exercises," *Journal of Homeland Security and Emergency Management*, 2025. <https://doi.org/10.1515/jhsem-2024-0039>

18 On the importance of not backing down, see Keir Giles, *What deters Russia Enduring principles for responding to Moscow* (Chatham House Research Paper, September 2021), 16, <https://www.chathamhouse.org/sites/default/files/2021-10/21-09-23-what-deters-russia-giles.pdf>

19 On this point see: Yevgeniya Gaber and Graeme P. Herd, "Russia's End State: What Deters Russia," George C. Marshall Center for Security Studies, Strategic Competition Seminar Series (SCSS), October 15 (2024): 4. <https://www.marshallcenter.org/sites/default/files/files/2024-12/fy25-sscs-1.pdf>

think like us or share our values. Here, we must recognise that some states have different strategic cultures, which make them hard to deter. Russian strategic culture is notable for its higher readiness to use force as part of a continuum of coercion, with emphasis on employing shock and deception and a greater willingness to risk casualties or losses.²⁰

Having a wide range of capabilities which are made obvious to the opposite force seems important in this context. Adversaries need to see that they are matched, if not potentially overmatched. In the Kerch Strait incident, the Ukrainians used lightly armed ships, which were probably viewed by the Russians as easy targets. Moreover, they were unsupported, whereas the Russians could deploy a network of assets, including fast jets.

As important as any physical naval hardware or legal software expertise, is the quality of leadership. Senior political decision-makers need to be confident in delegating to commanders on the spot to take the initiative, congruent with the principles of mission command, which Western militaries often aspire to but do not always achieve.²¹ One problem here is that senior civilian leadership may understand little about the value of mission command, and although historically navies typically empowered ship commanders with considerable discretion, more advanced networked systems have reduced some of the scope for naval mission command.²² The captain on the bridge is now being increasingly watched over their shoulder through real-time data links. Here, the temptation to micro-manage from a distant crisis room is both very real and likely counterproductive. Instead, what is required is a clear division of labour in leadership, tailored for the tactical, operational and strategic levels.

Levels of Leadership for A Hybrid Crisis at Sea

At the lowest level, the tactical commander at sea must typically share jurisdiction with several civilian agencies. Indeed, the lead actor may be a civilian maritime safety or law enforcement body working with navies and coastguards. In the Baltic, there are often multiple forces and agencies from different countries. There is a need to ensure very early on clarity and unity of command when facing a maritime hybrid threat: who is in charge at sea and of the incident overall?

The latter may not always be a vessel commander, as it could be a tactical commander on land or even in the air, who is best placed to manage all assets. This speaks to leadership of joint and multi-domain operations combining air, naval, special forces with cyber and police expertise. It is worth pointing out here that the Irish Naval Service has a track record of successful operations at sea, which have combined Army Ranger Wing and more often Garda and even Revenue Commissioners personnel in successful narcotics interdictions. However, hybrid operations involving hostile states may be considerably more challenging given their greater capabilities for use of force and escalation.

In any event, tactical and operational level leaders will typically have to exercise considerable discretion and judgement, including in detailed ways such as positioning of ships, or

20 See Dmitry Adamsky, *The Russian Way of Deterrence: Strategic Culture, Coercion, and War* (Stanford University Press, 2023), 102-108.

21 For a succinct overview of mission command in general, see: Anthony C. King, "Mission Command 2.0: From an Individualist to a Collective Model," *Parameters* 47, no.1 (2017).

22 On this specific point, see: Anthony C. King, *Command: the Twenty-First Century General* (Cambridge: Cambridge University Press, 2019), 451.

any employment of (less lethal) weapons or sensors. Of greater priority will be to keep communication channels open with simple and clear messages. And if the strategic intent of civilian leadership is unambiguously communicated to them, they can probably figure out very effective tactics to neither further escalate nor vacillate and reward aggression.

The actual handling of the situation at sea is one thing, its presentation and management in the information space is quite another. It is here that we can move to the operational and strategic levels. It is also here we conjure up the 'crisis room', which today features a watch floor with banks of screens and real-time data, fusing open source, social media and military channels. Arguably, these venues can easily become hot houses for information overload, which will be increasingly augmented by artificial intelligence tools pushing faster collection and analysis. Yet a higher speed or volume of data does not necessarily correlate with accurate intelligence analysis nor leaders taking good decisions.²³



Image is in public domain: <https://itoldya420.getarchive.net/amp/media/navy-cyber-defense-operations-command-watchfloor-825b59>

The 'watch floor' of US Navy Cyber Defense Operations Command circa 2010.

Indeed, any crisis room capability should come at the end of a long process of operational shaping and management of hybrid threats. The operational level should be about anticipating, and hardening vulnerabilities well before any incident can be engineered. In the example of the Kerch Strait incident, there was a year-long shaping campaign by the Russians, who claimed that Ukraine was spoiling for an escalation opportunity and they denied access to Ukrainian merchant vessels as part of a de facto blockade. At the operational level many hybrid threats are pretty obvious scenarios and should be no great surprise. The leadership question here is how such contingencies are planned for and in some cases deterred or mitigated by prior actions, deployments and doctrines.

What is left then for effective strategic leadership in such situations? Communication by political leadership is arguably critical. How they respond in the initial first few hours and the words they use greatly matter. In some cases, there is merit in 'strategic silence', especially where the facts are still murky, which is often the case at sea. A complicating issue here is coordination between international leadership, which may be required if the incident straddles adjacent maritime jurisdictions.

²³ For wider discussion see: Mikael Weissmann and Niklas Nilsson, "Current Intelligence and Assessments: Information Flows and the Tension between Quality and Speed," *International Journal of Intelligence and Counter Intelligence* 37, no.4 (2024): 1351-1367.

And while a high-level signalling of resolve may be called for, this is much more useful and achieves a deterrent effect if it is given well before a crisis occurs. Hostile actors need to be convinced that senior political leaders will authorise and empower relatively junior tactical commanders to act in ways that will either deny them the ability to carry out their threat or will (lawfully) punish them if they do so. Deterrence is usually considered to work when both attributes are credible. And high-level leaders also have a vital role to play in the prior shaping of the maritime domain through negotiating diplomatic agreements to provide deconfliction and manage incidents. These were a feature of the Cold War,²⁴ precisely to establish ground rules to avoid the use of force.

Learning or Forgetting Leadership Lessons?

In conclusion, this paper has explored leadership when facing maritime hybrid threats, focusing especially on shock, surprise, and decision-makers' overload, although these are more general problems applicable to many crisis scenarios. After observing how hybrid threats have developed in the Baltic Sea, a general maritime hybrid threat spectrum was also delineated. The point here is to underscore the range and diversity of the threats, from the lower to higher ends, the latter including considerable scope for violence.

Concluding sections explored how leadership can be made more resilient by paying attention to strategic communications and to the legal complexities which are often greater at sea. However, leadership when facing maritime hybrid threats needs also to move beyond communication to coordinating effectively: just enough to force key players out of their silos but not so overly hands-on as to stymie the necessary tactical flexibility of what will often be relatively junior or mid-ranking tactical level leaders.

We began this discussion with the Kerch Strait incident of 2018, but more recent incidents continue to provide much food for thought. For example, decisive leadership was shown by the swift response of the Finnish Border Guards to board and arrest the *Eagle S* on Christmas Day 2024. Yet such resolve only came after careful preparatory operational and intelligence analysis, including legal research well before the incident. Moreover, that vessel was essentially cooperative and compliant.

However, that benign reality is not guaranteed. In May 2025 when the Estonian Border Guard made an attempt to detain (but not board) a suspicious vessel (*MV Jaguar*), this was thwarted by an overflying Russian fast jet (Su-35). It circled as the merchant vessel in question simply ignored Estonian demands to stop and be checked. Arguably, this type of scenario should not have been a surprise and could have been anticipated. Yet it reveals how hybrid threats are becoming both increasingly commonplace at sea, and how they present a unique potential to both shock and paralyse Western states when faced either with actual violence or the likelihood of the same. Seven years on from the Kerch Strait incident, just how much have European democracies really learned, and how much has been forgotten?

²⁴ See David Frank Winkler, *Incidents at Sea: American Confrontation and Cooperation with Russia and China, 1945-2016* (Naval Institute Press, 2017).



Abstracts

7th Joint Command and Staff Course

Thesis Abstracts 7th Joint Command and Staff Course 2024-25

Submitted in partial fulfilment of the requirements for the MA (LMDS)

Maynooth University - 2024–2025

All theses are available on request from
the Defence Forces Library, Curragh Camp



**Maynooth
University**
National University
of Ireland Maynooth

Manual-Gaming and Maritime Operations Training – Educational Opportunities and Implementation Challenges for the Naval Service

Lt Cdr Donnchadh Cahalane

This study explores the contemporary use of manual-games (board games) in Professional Military Education (PME) and investigates their potential benefits and challenges in supporting maritime operations training within the Naval Service (NS). The NS has traditionally built decision-making and critical thinking skills through ‘at-sea’ experiential learning instead of formal classroom-based learning within the Naval College (NC). This model is threatened by a critical shortage of training berths within the NS fleet, owing to widely reported personnel shortages leading to the majority of ships being placed in an operational reserve state for the last six years. Manual-games, long acknowledged for their ability to enhance decision-making and critical thinking skills, offer a low-cost, realistic and effective solution to this critical and growing training gap.

A mixed-methods approach encompassing qualitative and quantitative research was employed to achieve the study’s aim. By conducting a survey, with responses from 127 currently serving NS personnel, and semi-structured interviews with both internal PME stakeholders and external experts, this study confirmed the significant dependence on informal sea-going experience for developing decision-making and critical thinking skills, while NS PME lacks effective structured delivery methods. Naval personnel indicated a high openness to adopting manual-gaming, especially after learning of its use by other western militaries. Key constraints, including limited resources, cultural perceptions and lack of experienced facilitators were also identified.

Manual-gaming offers a cost-effective, scalable, and adaptable solution for enhancing NS PME, which aligns with wider Defence Forces’ priorities for modernising training and improving joint operational preparedness. The study also presents a novel implementation framework, developed from the research findings, which connects learning objectives, delivery constraints, and game facilitation to support structured PME outcomes. To the author’s knowledge, this is the first study to specifically evaluate manual-gaming in the NS. It bridges a theoretical-practical gap in PME development, providing actionable recommendations for the integration of manual-games into NS PME with significant benefits for personnel development among all ranks and potential relevance across the wider Defence Forces.

Has the Closure of Defence Forces Barracks and the Reduction of the Reserve Defence Forces Impacted the Permanent Defence Force's Ability to Recruit?

Comdt Amy Colclough, B Comm, LLB.

In 1998, the strength of the Defence Forces (DF) was 11,653 Permanent Defence Forces (PDF) and 14,767 Reserve Defence Forces (RDF). In 2024, the strength of the PDF was 7,557 and the RDF was 1,720. Since 1998, 14 barracks have closed, and the Reserve Defence Forces has gone from having hundreds of locations to 28. This thesis examined whether the closures of barracks and a reduction in the RDF have had an impact on the PDF's ability to recruit, as the strength of the DF has been contracting for decades. The DF is currently in the process of metamorphosing; by 2028, it will have an establishment of 11,500. 2024 was the first time in seven years that the DF strength didn't decrease.

The methodology utilised an interpretivist approach to explore quantitative and qualitative data. Data on recruitment and strengths were collected from the Military Archive and the Recruitment Section. Data on motivators and influence on recruitment, including geographical considerations and the reserve, was generated from a semi-structured interview and a questionnaire.

The Research indicated that geographical downsizing of the DF has reduced visibility and community engagement, which has impacted the PDF's ability to recruit. The Reserve acted as a pathway for a career in the PDF; it provided visibility to the DF in rural areas, while the cadre staff had supported recruitment in these areas. The barracks closures and the 2012 reorganisation of the PDF have also impacted recruitment. Regional connections with the DF in certain areas are gone and the traditions of military service in these areas no longer exist. Increased commute affects work-life balance, which may impact willingness to choose a career in the PDF. Other militaries have identified the need to create connections with the community to generate a good work-life balance and foster recruitment. Most barracks being in urban centres also has implications. The cost of living is higher in these areas and there is greater employment competition from other sectors. The shift of appointments to the East has affected individuals from certain regions, as the decision to advance their careers in the PDF means becoming permanent commuters. Drawing on analysis of the literature reviewed and the evaluated data, the DF need to improve its visibility by creating connections with communities both in rural and urban areas to improve its ability to recruit.

Pay Or Passion? An Investigation into the Role of Pay As a Motivator for a Career in the Defence Forces

Comdt Shane Conlon

This thesis explores the complex interplay between financial remuneration and intrinsic motivation in influencing career choices within the Defence Forces. Drawing on both quantitative and qualitative survey data from current and former personnel, the study investigates whether pay acts as a primary motivator or merely a supporting factor when individuals decide to enlist and remain in military service. The research indicates the Defence Forces is not alone in facing these challenges, through the comparison of motivational factors in military careers to those in civilian sectors.

Findings reveal that while passion for service, patriotism and a sense of duty are significant initial drivers, dissatisfaction with pay emerges as a critical issue affecting long-term retention and morale. The study concludes that although passion may attract individuals to the Defence Forces, competitive and fair compensation is essential to sustain a committed and capable workforce. Recommendations are made for policymakers to balance intrinsic and extrinsic motivators to enhance recruitment and retention.

How Could Education Improve a Commander's Use of Sleep in Irish Defence Forces Operations?

Comdt Michael Conway, BSc, MSc.

This thesis investigates how education could improve a commander's use of sleep in Irish Defence Forces (DF) operations. While sleep is widely recognised as essential to performance and decision-making, it is rarely addressed in military leadership education or doctrine. Internationally in militaries, sleep-related education tends to be embedded within wellness programs, with limited application to operational planning or command-level decision-making.

This study combines a targeted literature review with qualitative interviews conducted with personnel across the Army, Air Corps, and Naval Service. The findings indicate that within the DF, there is no formal structure for educating commanders on sleep management. Most knowledge is acquired informally, through personal experience or civilian aviation protocols, and applied inconsistently during operations. Interviewees described instances where informal knowledge appeared to influence better use of sleep, suggesting that education may play a positive role when appropriately contextualised.

The research also highlights barriers to both delivering and applying sleep education. These include institutional norms that associate sleep restriction with toughness, limited manpower to support rest during operations, and a lack of integration between training, doctrine, and leadership practices. However, when education is supported by leadership modelling, practical planning tools, and doctrinal frameworks, it may help shift attitudes and operational habits.

The findings suggest that targeted, operationally relevant education could support commanders in recognising sleep as a critical planning factor. Integrating basic sleep science into leadership development and decision-making frameworks, such as the Military Decision Making Process (MDMP), may provide commanders with the knowledge and support necessary to balance performance and rest. While limited in scope, this study offers a practical perspective on how education could contribute to more sustainable operational effectiveness within the Defence Forces.

Ego and Command: To What Extent Does Ego Impact on Military Leadership Effectiveness

Lt Cdr Jamie Cotter

This study investigates the underexplored role of ego in military leadership effectiveness, addressing a notable gap in leadership scholarship in the process. Despite extensive research on leadership styles and emotional intelligence, the influence of ego on command performance in the military context remains underexamined. To bridge this gap, this study aims to determine how ego impacts leadership effectiveness in the Irish Naval Service.

A mixed-methods research design was adopted, integrating a quantitative survey with qualitative semi-structured interviews. This approach provided both measurable data and rich qualitative insights into leadership behaviours and decision-making processes.

The findings of this study reveal three key insights. First, ego has a dual effect on leadership showing that a balanced ego can enhance leaders' confidence, decisiveness, and overall effectiveness, whereas an inflated ego can undermine performance by fostering rigidity, arrogance, or toxic leadership traits. Second, current Naval Service leadership development has a blind spot regarding ego awareness, while existing leadership doctrine and training programs emphasise technical competencies and command skills, little attention is given to self-reflection and ego management. Third, participants widely recognised the importance of Emotional Intelligence (EI) and the associated soft skills in effective leadership, indicating that leaders who maintain self-awareness and check their ego are better able to foster trust and unit cohesion.

These findings have significant academic and practical implications. The study bridges psychoanalytic theory and military leadership practice by demonstrating how ego psychology concepts apply to leadership in hierarchical, military, high-stakes environments. It suggests that Naval Service leadership training and development should incorporate ego awareness and emotional intelligence components to cultivate more self-aware, adaptive leaders. The research application of psychoanalytic perspectives to military leadership, aims at offering a novel contribution to leadership theory and providing actionable recommendations to enhance leadership development within the Defence Forces.

“Be More”: Harnessing Sport and Fitness to Boost Recruitment and Retention in the Defence Forces

Comdt Pdraig Duggan, BA, MSc.

Since 2001, the Defence Forces’ strength has decreased by almost 30 percent, leading to a loss of expertise, capability and manpower. The Report of the Commission on the Defence Forces, published in 2022 appeared to be a watershed moment in how we, as an Irish society would perceive the defence of the state going forward, while opening the government’s eyes to the scale of the issues faced to achieve this.

Efforts have been made to improve the situation with the ongoing Detailed Implementation Plan reflecting increased spending on defence in areas such as infrastructure, capability and equipment. As stated in the DF White Paper our most important defence asset is our people. As such, every effort must be made to ensure recruitment and retention is optimised to get as many suitable people into the organisation and retain them in service through effective retention measures. This study does not purport to be a silver bullet in addressing these challenges; instead, it tries to identify the best method of harnessing sport and fitness to boost recruitment and retention in the Defence Forces.

A review of the literature explored the motivations for service in the military and how external factors e.g. economic conditions play a role; but also factors unique to an individual, such as adventure and values. The correlation between military service and sport showcased the strong bonds uniting both, with sport and fitness playing a significant role in attracting recruits. Concepts surrounding marketing were reviewed with the idea of linking how motivation, sport and fitness are harnessed to best effect during recruitment campaigns.

This study used a relativist lens to explore each participant’s unique perspective, while focusing on understanding different meanings constructed by individuals. This method of analysis required an interpretivist epistemological framework. To understand the meaning of this research in a coherent way, a thematic analysis of the primary research was conducted which included questionnaires (N=118), two focus groups (N=8 in each) and two semi-structured interviews.

Findings suggest sport and fitness are significant ‘pull’ factors into the organisation, however they are generally not decisive. Themes emerged during research that emphasise the role camaraderie and other intangibles specific to military service play in determining it as a career choice. The prevailing attitude among respondents was how the DF can better harness the ‘feeling’ military training provides, utilising sport and fitness to reinforce this. In this context, social media would play a key role, with suggestions brought forward as recommendations for the DF as part of any future advertising campaign.

The EWIPA Political Declaration: Policy Over Law in the Regulation of Explosive Weapons in Populated Areas

Comdt Ciara Gubbins, LLB.

The use of explosive weapons in populated areas continues to be a major cause of civilian harm in contemporary armed conflict. This research critically examines the 2022 Political Declaration on Strengthening the Protection of Civilians from the Humanitarian Consequences Arising from the Use of Explosive Weapons in Populated Areas (EWIPA) as a policy instrument that seeks to close the gap between legal obligations under International Humanitarian Law and operational military practice. The EWIPA Political Declaration is analysed as a form of ‘soft law’, a non-binding policy instrument that complements existing legal norms and promotes the implementation of avoidance-based practices to enhance civilian protection.

While not legally binding, its emphasis on standard-setting raises important questions about the efficacy of policy over law in regulating explosive weapons. This research examines the EWIPA Political Declaration as a policy approach and explores the legal and normative questions it raises in the regulation of the use of EWIPA. It considers the Political Declaration’s non-binding applicability alongside established International Humanitarian Law principles, with a focus on its potential to shape State behaviour, military practices, and evolving norms. This research seeks to contribute to understanding the Political Declaration’s potential to impact behaviours in armed conflict and the broader debate between policy and legal frameworks. The research also highlights Ireland’s central role in the Political Declaration’s development, situating its role within the broader context of principled neutrality, humanitarian diplomacy, and norm development. Ireland’s engagement demonstrates how small, neutral states can shape disarmament norms and exert influence despite lacking coercive power.

Ultimately, the research finds that the Political Declaration’s impact is constrained by fragmented implementation, inconsistent political will, and the ongoing erosion of respect for foundational IHL principles. This thesis concludes that while the Political Declaration is not intended as a substitute for legal enforcement, it offers a practical and politically viable path to enhancing civilian protection.

The Iraq War, Clausewitz, and the End of the Unipolarity

Comdt Seán Hanley

This thesis examines the US invasion of Iraq in 2003, through the lens of Carl von Clausewitz's theories on war, with particular focus on the trinitarian model of war, and the notion that "*war is merely the continuation of policy by other means.*" It argues that the Iraq War not only marked a strategic failure for the US but also served as the pivotal event that accelerated the end of the post-Cold War unipolar world order dominated by American hegemony.

Building on Charles Krauthammer's notion of the "*unipolar moment*," the research contends that the post-9/11 era presented the US with a unique opportunity to assert global leadership through the promotion of liberal democracy. However, by initiating the Iraq War based on ideological presumptions, flawed intelligence and tenuous legal justifications, and the U.S. rapidly squandered its legitimacy as a global hegemon. The study analyses how the Bush administration's strategy failed to align military means with coherent political objectives, leading to a quagmire that delegitimized American power both domestically and internationally.

The study examines Clausewitz's trinity—reason (government), chance (military), and passion (the people)—as an analytical framework to understand the disjointed nature of the war's rationale, conduct, and aftermath. The research highlights how the administration's reliance on exceptionalist rhetoric, underpinned by the 2002 National Security Strategy, alienated traditional allies and undermined multilateral institutions, that it paradoxically sought to uphold, yet simultaneously undermined. It demonstrates how the absence of clear and achievable political goals created friction, producing operational failures and a long-term insurgency that engulfed Iraq in civil war.

A second key argument examines the consequences of the US' misunderstanding of Iraq's ethnogeography and political culture. By imposing de-Baathification, disbanding the Iraqi military, and promoting a sectarian political system, the US inadvertently dismantled the state's ability to govern, resulting in a power vacuum and the rise of militias and insurgent groups. This chaotic transformation further undermined US claims to global leadership and exposed the dangers of applying neoconservative ideals to complex geographies that it proposed to shape and control.

Finally, the thesis assesses the broader geopolitical consequences of the Iraq War. It asserts that the failure in Iraq contributed directly to the erosion of U.S. influence in the Middle East, emboldened regional rivals, and diminished trust in American power worldwide. This strategic overreach is interpreted as the key inflection point that ended the unipolar era and ushered in a more volatile, multipolar global order.

Through critical analysis of primary and secondary sources, including political speeches, foreign policy documents, and other biographies and studies, this thesis contributes to our understanding of how Clausewitzian theory remains relevant in contemporary conflict analysis. It ultimately argues that the Iraq War stands as a study in the catastrophic misuse of military force in the absence of sound political judgment.

Controlling Chaos: Governance and Regulation of AI-Controlled Autonomous Weapon Systems

Lt Col Mario Heinz (Bundeswehr), MSc.

Based on intensive literature research and the evaluation of case studies, this thesis first explains necessary definitions, such as human-in/on/out of the loop, in order to then assess the real danger posed by the deployment of artificial intelligence (AI)-controlled autonomous weapon systems (AWS). To this end, the thesis focuses on the tactical, operational, strategic, but also ethical implications for future warfare. In current conflicts, such as those in Ukraine and Gaza, the development of this technology is advancing at an ever-faster pace. Without meaningful human control, tactical advantages such as speed, precision and adaptive behaviour lead to significant weaknesses in ethical frameworks such as international humanitarian law (IHL). One of the biggest challenges is the accountability gap as there are no laws governing who is responsible for the misconduct of an AI-controlled AWS. At the strategic level in particular such misconduct can lead to an AI security dilemma, which could further fuel geopolitical conflicts.

The thesis aims to use this information and, by combining it with a critical analysis of existing laws and regulations and an assessment of current power dynamics, to develop options for governing and regulating AI-controlled AWS. Due to global tensions and disagreements over definitions, the international community has not yet succeeded in developing a binding set of laws based on ethical standards or at least adapting existing laws to the deployment of AI-controlled AWS. For this reason, this thesis presents a tiered governance model that links the autonomy levels of AI-controlled AWS with traditional levels of warfare. Together with recommendations for implementation, this pragmatic model is intended to serve as a temporary solution for ethically conscious armed forces until it can be replaced by a more comprehensive, ethically grounded legal framework, ideally within the framework of international humanitarian law.

Quality, Readiness, and Retention: A Stakeholder Review of Ordnance Technician Training in Óglaigh na hÉireann

Comdt Jack Higgins, BSc, MEng.

This thesis evaluates the effectiveness of Ordnance Technician training within Óglaigh na hÉireann, focusing on the Army Ordnance Corps' Armourer stream. The study investigates whether current training syllabi meet professional standards, identifies areas for improvement, and explores factors influencing technician retention. Employing a mixed-methods approach, the research combines quantitative survey data from recently qualified and experienced technicians with qualitative feedback to provide a comprehensive assessment of training outcomes and readiness.

The findings indicate that while the syllabi deliver strong foundational competencies, particularly in frequently used skills such as small arms maintenance, there are notable deficiencies in less-practiced workshop skills (e.g., fabrication, milling, turning, welding) and administrative preparedness. Both new and experienced technicians report skill fade in these areas, attributed to limited practical exposure and insufficient ongoing training. Furthermore, the study identifies a disconnect between theoretical instruction and hands-on proficiency, highlighting the need for more structured mentorship, extended workshop modules, and regular refresher training.

Career satisfaction and retention are influenced by technicians' ability to apply their specialist skills and access career progression opportunities. Frustrations over routine non-technical duties and limited promotion pathways contribute to attrition, with some technicians seeking civilian roles where their qualifications are more fully recognised. The research underscores the importance of ongoing syllabus review, enhanced practical training, and administrative integration to maintain operational readiness and support technician retention. The thesis contributes to the academic understanding and practical advancement of military technical training in Ireland, offering actionable recommendations for curriculum updates, mentorship structures, and administrative reforms. It also highlights the need for continued research, including benchmarking against international standards and longitudinal studies on skill retention. Ultimately, the study advocates for a dynamic, responsive training system that meets evolving Defence Forces requirements and supports the professional development of its technical personnel, thereby supporting the safe conduct of Military Training and operations into the future.

“True Grit”: Investigating Resilience and Dropout Risk among Gen Z Recruits in the Irish Defence Forces

Comdt Ruaidhrí Kedney

This thesis examines the non-cognitive psychological traits of grit and hardiness and their association with training attrition among Irish Defence Forces (DF) recruits. Framed against the backdrop of the DF recruitment and retention crisis and persistently high dropout rates during induction training, the research tests the hypothesis that low levels of these traits correlate with an increased likelihood of training failure. Informed by the frameworks of Bartone and Duckworth, this study adopts a quantitative, cross-sectional survey design.

Data from DF recruits ($n = 65$) were collected immediately following attestation during Q1 2025. The research employed the validated self-report instruments of the 12-item Grit Scale and the 15-item Dispositional Resilience Scale (DRS-15). Descriptive statistics established baseline profiles, while inferential analyses—including t -tests, effect sizes, and Pearson’s correlations—explored differences between recruits who completed training and those who dropped out, as well as the relationship between grit and hardiness.

Key findings indicate moderate to high levels of grit and hardiness within the entire research cohort. A modest association was also observed between lower grit scores and an increased likelihood of early-stage training attrition. No statistically significant relationship was identified between overall hardiness and dropout rates. Finally, despite their distinction as noncognitive psychological traits, a strong correlation was found between grit and hardiness constructs. Although the study was constrained by its cross-sectional design and sample size, limiting its generalisability, the thesis recommends incorporating non-cognitive trait testing into the recruitment process. The DF may benefit from further longitudinal research to elucidate the predictive value of grit and hardiness concerning personnel retention and performance prediction.

Do Enlisted Pte Soldiers of the Irish Defence Forces Practice Courageous Followership and to What Extent Is This Encouraged by Military Leadership?

Comdt Edward McAuley, BComm.

This thesis investigates the extent to which enlisted Private (Pte) soldiers (OR-2/3) in the Irish Defence Forces (DF) practice courageous followership and whether these behaviours are encouraged by military leadership. Given the recent DF efforts to modernise its culture and in support of the DF Strategic Transformation 2023 agenda the research identifies a significant gap by focusing on the largest cohort of personnel in the DF enlisted Pte soldiers whose lived experiences have been underexplored and investigated.

The literature review draws from leading academic frameworks in the field of followership including Kelley's typology of follower, Chaleff's courageous followership model and Kellerman's engagement spectrum. These theories are critically examined along with military doctrines from the DF, the British Army and the New Zealand Defence Forces. The review identifies gaps in DF training and cultural barriers that continue to prevent ethical dissent and initiative among enlisted Pte Soldiers.

Adopting a qualitative, hermeneutic phenomenological methodology, data were collected via one focus group and three semi-structured interviews with DF personnel across a range of ranks. Thematic analysis revealed five core themes that included (1) varied understandings of followership, (2) how leadership style influences organisational culture, ethical dilemmas and (3) the role of transformation, (4) how experience and confidence contributes to courageous followership behaviour, and (5) the existence of informal mentoring methods that encourage this behaviour without formal education in the area.

The findings suggest that while elements of courageous followership do exist, they are inconsistently practiced and poorly supported by formal training. Enlisted Pte soldiers lack a shared understanding of followership concepts, respectful challenge and taking moral action remains constrained by the culture. The research concludes that enhancing doctrine, supporting leadership development in followership and the introduction of followership education at the induction or Three Star training level to promote courageous followership behaviours.

The research contributes original insights into civil-military relations, ethical leadership and cultural reform in the DF. It proposes actionable recommendations to enhance followership behaviours amongst Pte Soldiers that will permeate through to support our future leaders while aligning with Ireland's defence transformation agenda.

Contested Manoeuvre in Large Scale Combat Operations: Confronting Manoeuvre Denial in Multi-Domain Operations

Maj James F. McAuliffe (U.S. Army)

The return of great power conflict and rapid proliferation of advanced artificial intelligence, unmanned vehicles, and other technologies amongst state and non-state actors present evolving strategic challenges for the United States and its allies. Contemporary strategic discourse has centred on the multi-domain threats Anti-Access and Area Denial (A2/AD) systems pose. This emphasis on A2/AD systems has obscured broader developments in denial-based strategies. National policy, military planning, and academic discourse fail to address these broader vulnerabilities, leaving U.S. strategic planning unprepared for the future of large-scale combat operations (LSCO).

This paper examines a critically assesses a central research question: how should the U.S. Army Engineer Regiment in a resource constrained environment transform to mitigate the emergence of sophisticated ground manoeuvre denial strategies? It challenges Western militaries' assumptions surrounding the current ability to manoeuvre forces unimpeded, a principle known as Freedom of Maneuver (FoM). This paper examines three lines of inquiry: the evolution of manoeuvre denial as a strategic threat, reframing manoeuvre denial within the operational environment (OE), and prioritization of investment to mitigate the threats of manoeuvre denial. For the purposes of this paper, manoeuvre denial is reconceptualized, expanding the understanding of denial as a broad and inherently multi-domain challenge and positioning the concept as a critical subset.

An author-developed framework synthesizes deductive-inductive logic and problematization to assess if manoeuvre denial qualifies as a strategic threat. Findings are evaluated through the U.S. Army's Assured Mobility Framework (AMF) to diagnose operational challenges manoeuvre denial poses to Freedom of manoeuvre, especially as the Engineer Regiment is downsized.

The paper's findings validate the proposed framework and demonstrate that manoeuvre denial poses a strategic threat to FoM. Targeted investments in AI and unmanned ground vehicles reduces operational risk and mitigates the impact of force reductions across U.S. and allied forces. Ultimately, understanding and addressing denial-based threats is central to preserving the strategic initiative in future LSCO.

The Future of Lessons Learned within the Irish Defence Forces: Nesting, Roles and Methodology

Comdt John Moody

This thesis is titled ‘The future of lessons learned within the Irish Defence Forces: Nesting, roles and methodology’ and it explores the crucial role which lessons learned plays, and how it is positioned, within the Irish Defence Forces (DF). It also proposes a transformative approach which could optimise the architectures and structures which underpin the discipline in the future.

The study identifies significant gaps in the current positioning or ‘nesting’ of lessons learned functions within the DF and examines the roles and methodologies employed in capturing, analysing, and disseminating lessons. This thesis advocates for a more strategic and integrated approach to lessons learned within the DF, greater alignment with NATO best practices and ensuring high command authority.

The thesis identifies two primary challenges within the DF’s current lessons learned framework: the inadequate nesting of the function within the Directorate of Defence Forces Training, J7 and the need for enhanced roles and methodologies. The research examines the historical context of the DF’s lessons learned process and critiques its current structure against international standards.

This paper’s introduction underscores the importance of learning from past experiences as a fundamental component of military success and draws on contemporary examples. The literature review highlights contributions from key scholars and institutions, particularly NATO’s Joint Analysis & Lessons Learned Centre, which serves as a benchmark for best practices in organisational learning.

Chapter One delves into the existing systems and practical implementations within the DF and NATO, highlighting the limitations of the DF’s training-centric approach. The chapter proposes a re-evaluation of the DF’s lessons learned function, advocating for its repositioning under the direct authority of the Chief of Staff to enhance command authority and strategic visibility.

A critical analysis of the performance of both the DF and NATO systems, emphasising the importance of high-level command ownership in driving organisational learning is delivered in Chapter Two. The study reveals inefficiencies within the DF’s current framework and proposes alternative structures to maximise the system’s effectiveness.

The final chapter outlines a comprehensive framework for transforming the DF’s lessons learned architecture. Recommendations include repositioning the function within the COS’s office, integrating lessons learned training into existing courses and leveraging

future technologies such as AI to enhance data collection and analysis. The chapter also considers the potential impact of the proposed 2022 'Report of The Commission on The Defence Forces' on the DF's organisational structure. By implementing these recommendations it is hoped that the DF can foster a culture of continuous improvement and enhance its operational effectiveness and capacity to meet the challenges of the future.

Cultural Change in the Irish Defence Forces: A Unit Commander's Perspective

Comdt Denis O'Brien, MSc HRM

This study explores the perspectives of Unit Commanders within the Irish Defence Forces (DF) regarding their role in designing and implementing cultural change and examines a potential weakness in the current approach, a predominantly top-down implementation strategy that may not fully empower leaders at the tactical level to initiate cultural change within their units.

A mixed-method approach was used to initially gather data on the perceptions of Unit Commanders towards cultural change, followed up by qualitative research through a series of interviews which facilitated this understanding, allowing for a thorough exploration of the topic. The research findings suggest that the DF possesses an organisational culture characterised by a strong sense of community and camaraderie with an ingrained resistance to

external scrutiny. Unit Commanders place high importance on traditions and discipline but are struggling to implement cultural change at unit level due to three interconnected factors, namely resource constraints, communications gaps, and leadership challenges. Resource constraints undermine Unit Commanders efforts to implement cultural change initiatives while meeting existing operational commitments. Communication gaps amplify the disconnect between the strategic and tactical levels, while leadership challenges, rooted in insufficient training in cultural change management, limit the Unit Commanders ability to drive change within their Units. Cumulatively, the three factors present significant barriers to cultural change at the Tactical Level.

This study offers actionable recommendations to enhance the DF Cultural Change implementation, including addressing the resource constraints, enhancing communications and strategic alignment, and investing in leadership training in cultural change management

Stronger Together: How Can the Defence Forces Leverage Defence Standardisation to Enhance Its Interoperability with Partners?

Comdt Eoin O'Brien

Defence standardisation plays an important role in modern military operations, with its primary goals centred on enhancing interoperability, improving resource management and boosting operational effectiveness. This thesis analyses the current state of defence standardisation within the Irish Defence Forces and examines how defence standardisation can be leveraged to build military capabilities that are interoperable with regional partner nations.

This thesis utilises DOTMLPF-I and DOTmLPF-P as frameworks from which to examine three main questions. Firstly, what is defence standardisation, what are its aims and potential impacts on the Defence Forces? Secondly, how does the current defence standardisation landscape within the Defence Forces function? Thirdly, how do European partners manage defence standardisation, and what lessons can the Defence Forces adopt to enhance governance, implementation, and engagement?

Through the examination of the current state of defence standardisation it identifies three key areas that the Defence Forces can work on to improve standardisation implementation and its end state of interoperability. These three areas include weak governance, ineffective implementation and inconsistent engagement. This thesis examines options to address this through an analysis of partner's governance structures and mechanisms, implementation planning and management and standardisation engagement and understanding.

Finally, it suggests a tailored solution for the Defence Forces to address the areas outlined above based on the experience and knowledge of the Defence Forces European partners. The thesis concludes by identifying standardisation as a key tool that allows for the development of a firm foundation from which to build military capabilities that are interoperable with its European partners.

Irish Naval Service Recruitment and Retention Crisis

Lt Cdr Diarmaid O'Donovan

This thesis examines the recruitment and retention crisis facing the Irish Naval Service (NS), a situation that has critically undermined its operational capability. From a peak strength of 1,090 personnel in 2016, numbers have declined to 719 by 2025, a 33 percent reduction that has left the NS unable to crew several vessels and fulfil its operational roles. Through quantitative analysis, this study investigates the multifaceted causes behind this decline, including operational tempo, pay and conditions, changing societal attitudes towards military service, and failures in both recruitment strategies and retention policies.

Drawing on primary data, government reports, and comparative studies of foreign militaries, the thesis highlights that recruitment efforts have not yet compensated for departures, particularly among specialist technical personnel. Retention has emerged as the more pressing issue, exacerbated by outdated personnel policies, loss of pension incentives, limited career progression, and attractive civilian employment alternatives. The thesis finally examines public perception, shaped by both high-profile humanitarian missions and damaging scandals, and how this also plays a critical role in shaping enlistment trends and institutional morale.

While recent policy interventions including improved pay, expanded recruitment campaigns, and outsourced recruitment efforts represent attempts to reverse the decline, they remain piecemeal and inadequately focused on retention. Drawing on international best practices, this thesis recommends a strategy centred on personnel welfare, institutional culture, and career sustainability.

Ultimately, the research argues that the NS cannot rely on recruitment alone to restore its strength. Instead, a strategic pivot is needed, one that views service members as a long-term investment and prioritises their retention as a core pillar of national maritime security. Without such reform, Ireland risks the continued erosion of its naval capabilities at a time of growing geopolitical instability and increasing demands on the Naval Service.

Leadership in the Age of Artificial Intelligence: Navigating the Moral And Ethical Complexities of Autonomous Systems in the Defence Forces

Comdt Rónán O’Flaherty, BSc, MSc.

This thesis analyses the ethical challenges and leadership implications posed by the integration of Artificial Intelligence and autonomous systems into the Defence Forces’ command and control structures. Recognising the strategic backdrop of the evolving geopolitical landscape and dynamic nature of cyberspace, this research examines how military leadership can adapt to maintain ethical values, accountability and operational effectiveness as it seeks to embrace emerging and disruptive technologies. Through detailed analysis, case study evaluations and critical engagement with the latest research, particularly targeting and cyberspace operations, the study reveals a persistent tension between technical efficiency and ethical responsibility. This research identifies three central challenges: the erosion of human judgement in military decision-making, the attribution problem regarding cyberspace operations and autonomous systems, and lacunae surrounding leadership doctrine in addressing these challenges. Case studies illustrate the consequences of reduced human agency in targeting decisions. The thesis presents the Collateral Effects Estimate Process as a viable tool to assist the commander in assessing the impact of AI-enabled operations. Key recommendations include the creation of a dedicated Artificial Intelligence oversight section within the Joint Cyber Defence Command, a revision of the leadership framework to include human-AI interaction, and the formulation of a policy for accountability that will be consistent with International Humanitarian Law. Artificial Intelligence has the potential to be either a strategic multiplier or a liability; this thesis argues for a proactive response to ensure that operational benefits are consistent with ethical values.

Building For The Future: National And International Perspectives On Defence Infrastructure Modernisation

Comdt Kevin O'Reilly BEng, MSc, CEng MiEI

This thesis examines the infrastructure maintenance and development practices of the Irish Defence Forces (DF), evaluating their effectiveness in comparison with selected national estates and international defence estate organisations. In light of the significant challenges facing the DF estate, the research identifies key inefficiencies and explores opportunities for improvement. Adopting a qualitative case study approach, data was gathered through semi-structured interviews with national and international infrastructure professionals, supported by a review of relevant literature.

The findings highlight several strengths, including the ongoing development of installation masterplans, an effective Infrastructure Development Plan, internal design capabilities and the strategic use of consultancy frameworks. However, critical gaps remain—most notably the absence of a unified estate policy framework, including a dedicated estates strategy and maintenance policy. Infrastructure responsibilities are fragmented between the Department of Defence and the DF, funding for both capital works and maintenance is inadequate, and IT limitations hamper modern estate management.

Comparative analysis with New Zealand and UK defence estate models reveals more integrated and efficient organisational structures that could inform reorganisation in Ireland. Based on these insights, the study presents actionable recommendations for DF and Department of Defence leadership, including the creation of a unified infrastructure organisation, the development of a comprehensive estate strategy, the ring-fencing of capital infrastructure funding and the digital transformation of estate functions.

This research contributes to the limited discourse on defence infrastructure management by providing practical, evidence-based recommendations to enhance efficiency. It underscores the urgent need for long-term planning and policy reform to ensure the DF estate is sustainably managed and aligned with strategic defence objectives. Ultimately, the study offers a modernisation framework informed by best practices.

Fog Or Friction: An Examination of Civil-Military Relations Amongst Middle Managers Within the Irish Defence Nexus

Comdt Kenneth O'Rourke BA, MA

This thesis investigates civil-military relations (CMR) in Ireland by examining the professional interactions between middle managers in the Department of Defence (DoD) and the Defence Forces (DF). Within the unique context of Ireland's dual governance structure, the research explores how institutional ambiguity affects policy delivery, strategic coherence, and the ability of middle managers to fulfil their roles effectively. Using a modified conceptual framework derived from Bruneau and Matei (2008), the study analyses four dimensions: Civilian Control, Effectiveness, Efficiency, and Alignment. The research adopts a qualitative interpretivist methodology, employing semi-structured interviews, focus groups, and documentary analysis. Data were thematically analysed using Braun and Clarke's (2006) six-phase model, followed by deductive categorisation using the conceptual framework.

Findings reveal deep-rooted cultural divergence between the DoD and DF, driven by contrasting organisational norms, professional identities, and decision-making practices. While formal political control is accepted by the military, policy ambiguity and fragmented communication hinder effective coordination at the strategic-operational interface. Middle managers frequently operate in silos, constrained by unclear roles and limited institutional connectivity.

Notably, the study finds that interpersonal rapport and informal networks play a critical role in bridging these CMR gaps, enabling operational workarounds despite structural barriers. This thesis offers a balanced and transparent analysis, making an original contribution by characterising the cultural and organisational dynamics shaping Irish CMR. It concludes with recommendations for governance reform, clarified role structures, and a renewed emphasis on shared strategic purpose. The findings have relevance for Irish defence policy and broader small-state CMR contexts.

“Unseen Assets”: Leveraging Neurodiverse Talent As a Force Multiplier for Operational and Organisational Effectiveness

Comdt Rory Patrick Quinlan PG Dip.

The aim of this thesis was to examine how the Defence Forces can harness the strengths and abilities of neurodivergent individuals to enhance organisational and operational effectiveness. With 15–20 percent of the general population as neurodivergent, the Defence Forces could capitalise on the skills that these individuals could bring to the organisation. To truly be reflective of the society it serves the Defence Forces will need to look beyond the typical to the atypical.

A mixed-methods approach was undertaken in this study which encompassed qualitative and quantitative research methods. Through the conduct a workplace survey and semi-structured interviews, this study identified important themes that helped to garner valuable insights for integrating neurodivergent individuals into the Defence Forces. The research findings indicate that there is a lack of awareness and understanding of neurodiversity in the Defence Forces across all ranks which obstructs the integration of neurodivergent individuals into the organisation. While a limited awareness exists, the study emphasises the need for neurodiversity education and training of all personnel. The study also highlighted several barriers that must be addressed to improve integration. These include stigma, bias and fear related to disclosure, the lack of formal policy on neurodiversity, resistance from existing personnel, the *“soldier first principle”*, rigid career pathways and recruitment and selection practices.

This study offers recommendations that can enhance the Defence Forces organisational and operational effectiveness, including awareness campaigns, targeted training modules, guidance and policy mechanisms, development of specialist roles, career streams and civilian career pathways. By implementing these recommendations, the Defence Forces can increase its organisational and operational effectiveness while also being an organisation that truly reflects the society it serves.

Bridging the Gap Between Ambition and Architecture: Assessing Data Analytics Maturity and Strategic Enablers for Digital Transformation in the Irish Defence Forces

Comdt Gary Walsh, MSc (Data Analytics)

As technology becomes increasingly integral to military operations, data and analytics are emerging as crucial components in enhancing decision-making. Consequently, military organisations have recognised the strategic significance of data architecture and analytics. This thesis examines the current state of data analytics maturity within the Irish Defence Forces and the strategic enablers necessary to cultivate a data-informed organisation. The research is divided into three distinct phases: exploration, design, and evaluation. In the exploration phase, the study adopts a macroscopic lens, focusing on the conceptual, organisational, and technological factors that drive the integration of analytics within military contexts. The design phase examines the requirements for developing a practical framework for data analysis, concentrating on identifying the core dimensions needed for an analytically capable military. The evaluation phase applies this theoretical framework to the Irish Defence Forces, utilising both qualitative and quantitative data to assess and determine the current state of analytical maturity within the Defence Forces. Findings from this phase identify significant gaps in the Defence Forces' existing data architecture. Most notably, access to accurate and timely data, along with the persistence of siloed systems, are key barriers limiting the Defence Forces' ability to advance its analytical capability. The final part of the thesis consolidates the findings by presenting a phased implementation roadmap and offering strategic recommendations to guide the Defence Forces in enhancing their data analytics maturity.



Contributor Biographies

Zurab Bezhanishvili. Mr Bezhanishvili is an independent researcher and public administrator with over two decades of experience in national security, civil-military cooperation, and strategic development. He is the Founder and President of the International Community for Georgia Development and Progress and an alumnus of the Geneva Centre for Security Policy (GCSP). Mr. Bezhanishvili's professional background spans critical areas including hybrid threats, crisis management, counterintelligence, and defence planning, with a focus on the Black Sea, MENA, and Eurasian regions. He has conducted extensive fieldwork on the impact of disinformation, cyber operations, and the erosion of institutional trust during periods of war and instability. His interdisciplinary expertise draws from academic training in public administration, political analysis, and law, and is informed by on-the-ground experience during pivotal crises in post-Soviet Georgia. Currently, he is focused on advancing research into the doctrinal and leadership challenges posed by the post-truth security environment, emerging technologies, and information warfare. His work emphasises values-based leadership, democratic resilience, and strategic innovation in the face of evolving hybrid threats. Mr Bezhanishvili contributes to scholarly and policy discussions at the intersection of military leadership, international security, and technological transformation in contested geopolitical contexts.

Lieutenant Colonel Brian Cahill. Lt Col Cahill is an infantry officer with over twenty-four years of service in the Irish Army. He has extensive operational experience, having deployed on eight overseas missions to Liberia, Kosovo, Western Sahara, Syria, and Lebanon. His appointments have spanned a range of command and staff roles both at home and abroad, contributing to tactical operations and strategic planning as well as delivering professional military education as an instructor in the Military College. Lt Col Cahill is a graduate of the 6th Joint Command and Staff Course and holds an MA in Leadership, Management, and Defence Studies, an MSc in Intelligence and Security Studies, and a BA in History and Psychological Studies. Elements of his DF Review article are extracted from his MA thesis titled "Preparing for the Concrete Jungle - Adapting Irish Army Doctrine and Training for Urban Operations." Lt Col Cahill is currently serving as a senior staff officer in the Transformation Management Office in Defence Forces Headquarters.

Commandant Killian Doyle. Comdt Doyle is a Communication and Information Services (CIS) officer with 13 years of service in the Irish Army. His appointments have included a variety of command, staff, and technical roles at home and overseas, including serving in a brigade field CIS company, the Defence Forces Headquarters CIS company, and as signals officer and S1 of a deployed infantry unit in the Golan Heights. Comdt Doyle has over four years of experience with the Computer Incident Response Team (CIRT), exposing him to cyber defence at the tactical and operational levels. He has also made numerous contributions to strategic-level capability development. Comdt Doyle has several technical qualifications, including two MScs as well as a higher diploma in Leadership, Defence, and Contemporary Security. His professional areas of interest are Cyber Threat Intelligence (CTI) and behavioural security.

Corporal Fearghal Fitzgibbon. Cpl Fitzgibbon is a primary school teacher in Kerry and but is also a reservist NCO currently serving in the Army Reserve with 12th Infantry Battalion. Cpl Fitzgibbon holds a BA (Hons) in English and History from the University of Limerick and a Master of Education degree from Hibernia College, Dublin. He has also completed academic programmes with the University of Salzburg in Austria.

Dr Brendan Flynn. Dr Flynn is a Senior Lecturer/Associate Professor at the School of Political Science and Sociology, University of Galway, and currently serves as the head of political science. He teaches a wide range of undergraduate and postgraduate courses on European politics, Ocean and Marine politics and Conflict, Security, and Peace studies. His research lies at the intersection between maritime security and resilience with respect to energy transition and climate change challenges, including expertise on defence and security matters more generally. Dr Flynn is a regular media commentator on political and security developments and has contributed as a guest lecturer to several iterations of the Irish Defence Forces Joint Command and Staff Course and the Irish Army's Land Command and Staff Course.

Corporal Yvonne Kearney. Cpl Kearney has over 27 years of service in the Irish Army. She has previously served in 1 Brigade Headquarters in a variety of staff functions, including operations and as the brigade legal clerk, while concurrently championing coaching and mentoring in the organisation for over a decade. She has deployed overseas on operations on several occasions, including tours to UNIFIL (Lebanon) and KFOR (Kosovo). She holds a BA (Hons) in Counselling and Psychotherapy, an MSc with First Class Honours from UCC in Personal, Business and Executive Coaching, an MA with First Class Honours in Teaching and Learning in Higher Education from SETU, a Postgraduate Diploma in Workplace Wellbeing from Trinity College Dublin, and a Diploma in Mentoring from Kingstown College, Dublin. Professional body memberships include the Irish Association for Counselling and Psychotherapy (MIACP), the British Psychological Society (BPS), the European Federation of Psychologists Association (EFPA), Senior Level Individual Practitioner (EIA) and Senior Level Programme Manager (IPMA) with the European Mentoring and Coaching Council Global (EMCC). Cpl Kearney currently serves in Strategic Human Resources Division, Defence Forces Headquarters, as the first ever Coaching and Mentoring Programme Manager.

Commandant Simon Keenan. Comdt Keenan is an instructor in the Command and Staff School, having led on the Joint Command and Staff Course Operational Planning and Strategic Studies modules. His 21 years' service includes operational tours with the UN and the EU and a variety of domestic command, training, and staff appointments. His primary degree was a BSc in Design. He also holds an MSc in Security and Risk Management from the University of Leicester and an MA in Defence Studies from King's College London. He is a graduate of the UK's Advanced Command and Staff Course and has recently completed a course in Alternative Analysis.

Battalion Sergeant Major Shane McEneaney. BSM McEneaney is an infantry NCO with 24 years of service in the Irish Army. He has served in a variety of leadership and staff roles, including appointments in the 5th and 27th Infantry Battalions, and 2 Brigade Headquarters at home. He has also completed seven operational deployments to KFOR (Kosovo), UNMIL (Liberia), UNIFIL (Lebanon), EUFOR Chad, and EUTM Mali. He is currently deployed with the European Union Battle Group Force Headquarters at EUROCORPS Headquarters, Strasbourg, France, where he serves as the CJ3 cell senior enlisted advisor. BSM McEneaney holds a BA in Leadership, Management, and Defence Studies with Distinction from South East Technological University, an MA in International Security and Conflict Studies with First Class Honours from Dublin City University, and he is currently studying for an MA in Strategic Studies from University College Cork. BSM McEneaney has a keen interest in geopolitics and rugby. Prior to his deployment to Strasbourg, he was an active rugby coach for the combined Defence Forces / Garda women's rugby team.

Sergeant Stephen McCabe. Sgt McCabe is an Air Corps NCO with 21 years of service in the Irish Defence Forces. He began his career with the Army's 27th Infantry Battalion and later served with 2nd and 7th Infantry Battalions before transferring to the Air Corps in 2021. Sgt McCabe has extensive experience in training and educating inductees and junior leaders, particularly in the area of leader development, which he is quite passionate about. His achievements include a qualification in Change Management from University College Dublin and graduation from the inaugural NATO NCO Leadership Course. Leadership has always been a strong personal interest for Sgt McCabe, manifested by extensive independent reading on the topic. Outside of the Defence Forces, Sgt McCabe has been heavily involved in rugby as a player, captain, and youth coach. He currently serves with No. 5 Support Wing as the NCO-in-charge of base security at Casement Aerodrome.

Brigadier General Brendan McGuinness. Brig Gen McGuinness has served in the Irish Army for over 40 years and is currently General Officer Commanding the Defence Forces Training Centre. Recent appointments include Commander of Joint Task Force and Director of Operations and Plans in Defence Forces Headquarters. Previous appointments include School Commandant, Infantry School and Director of Infantry, Commandant Military College, Headquarters Support Group Commander, KFOR (Kosovo), Officer Commanding the 51st Infantry Group, UNIFIL (Lebanon) and Officer Commanding 7th Infantry Battalion and Cathal Brugha Barracks. Currently, Brig Gen McGuinness has a role in influencing and progressing work on Army Force Design and the Armoured Fleet Programme. Brig Gen McGuinness is passionate and active in developing and implementing Coaching and Mentoring approaches and programmes as part of Defence Forces leadership doctrine and practice. During his career, Brig Gen McGuinness has served with the UN, EU, NATO PfP and, the Organisation for Security and Co-operation in Europe (OSCE) in a wide range of military and non-military roles. He holds an MSc in Executive Coaching from Smurfit Business School, UCD. He is also a graduate of the Military College with an MA in Management, Leadership, and Defence Studies from Maynooth University.

Commandant Tadhg O'Donoghue. Comdt O'Donoghue joined the Irish Army in 2004 as a member of the 81st Cadet Class and was commissioned as an infantry officer to the 4th Infantry Battalion. Since commissioning, he has served in a range of appointments at home and overseas, including postings to 1 Bde Headquarters, the Directorate of Operations and Plans, the Joint Task Force, and Sector West Headquarters, UNIFIL (Lebanon). He is currently serving as an instructor in the Command and Staff School, Military College. He holds an MSc and Postgraduate Certificate from University College Cork, an MA from King's College London and is a graduate of the UK Advanced Command and Staff Course.

Dr Dennis Vincent. Dr Vincent was commissioned into the British Army, serving 30 years and taking part in many major campaigns. He was awarded an MBE for his leadership on operations, and his last tour of duty was as Colonel Training at the Royal Military Academy Sandhurst. He left the Army in 2015 to become the Head of the Department of Communication and Applied Behavioural Science at the Royal Military Academy Sandhurst, a post he conducted for nine years, before joining Cranfield University. His main role at Cranfield University is delivering the Strategic Leadership Programme course, deploying world-wide. He has a PhD in Military History and Leadership Studies from King's College London, an MA in Military Ethics also from King's College London and an MSc in Leadership and Management from Portsmouth University. His first book *The Forgotten General: General Sir Alan Cunningham*, focused on operational and strategic leadership and was runner-up in the Templar Prize for best new book in 2024. His second book *The S-CALM Model: The Application of Ethical Leadership in the Military* focuses on applied military ethics. He is a Chartered Manager, a Fellow of the Chartered Management Institute and a Fellow of the Higher Education Authority



DFPP

DFPP_JN_18683_25/300