Transforming Joint Air and Space Power

THE JOURNAL OF THE JAPCC

Edition 40 | 2025

Joint Air Power Competence Centre

Protector RG Mk1

Gambit Series

POWERING RPA INNOVATION FOR THE WORLD'S TOUGHEST MISSIONS

We deliver remotely piloted aircraft innovation powered by experience, ingenuity, and performance — backed by world-class partners.

That means unmatched pole-to-pole strategic ISR from the multi-mission, long-endurance MQ-9B. For short takeoff and landing in the most austere environments, deploy our groundbreaking MQ-9B STOL. And for the best all-domain awareness deep within the battlespace, look to our jet-powered Gambit Series combat aircraft.

These next-gen solutions deliver affordability at scale for any mission anywhere. And they're ready today.

MQ-9B STOL

Scan to learn more

ISR 24/7

Enabling Information Dominance

GENERAL ATOMICS
AERONAUTICAL

Editorial

Welcome to the 40th edition of the JAPCC Journal. As we continue to mark our 20th Anniversary this year, we are taking the unique opportunity not only to reflect on two decades of progress in Alliance Air and Space Power, but more importantly, to look ahead to the challenges and opportunities on the horizon. This edition, therefore, explores the critical adaptations NATO must embrace to deter and defend for decades to come.

I'm excited about the articles in this edition, where we directly confront the need to evolve our thinking, technology, and structures. You will find this theme explored through the lens of strategic foresight in our article on *Wargaming,* a critical tool for testing and refining future concepts and force design. We also examine the intellectual core of modern warfare with a fresh look at *Digitized Targeting* and the imperative of *Evolving C2 for Decisive Air Power,* where guest authors recommend how to best orchestrate effects across all domains to prevail.

This adaptation is driven by a blend of technology and integration. Several articles tackle the disruptive capabilities shaping the modern battlespace. We offer an operator's perspective on the immense potential and practical challenges of *Hypersonics,* and examine the transformative role of *Artificial Intelligence* in enhancing the training of our air battle managers.

Our front page and main article are dedicated to the first of three inside stories about the major sixth generation fighter programmes within NATO and Allied countries. Here we begin to look ahead to the next generation of air power, with a contribution from the *Global Combat Air Programme (GCAP).*

Yet technology alone is not enough. As John Boyd used to say: *'People, Ideas, and Hardware, in that order.'* Success depends on our ability to integrate these capabilities together. Our article on *Space-Centred Leadership* addresses the unique traits our Space leaders will need to succeed in this important domain. We then focus on ongoing advancements of NATO's *Air-Land Integration,* and we've also considered the full spectrum of warfare, from revitalizing NATO's *Personnel Recovery* mission, to strengthening our *Civil-Military Cooperation in the Cyber Domain.* Finally, we ground these future-focused discussions on the realities of today. An analysis of *Electronic Warfare Challenges in the Russia-Ukraine War* provides lessons for the Alliance.

I am proud of the work our JAPCC team and guest authors have invested in this edition to provide an intellectual foundation for the Alliance. These discussions will continue at our upcoming *Joint Air and Space Power Conference,* where we look forward to engaging with you in person. We hope you find this collection of articles both thought-provoking and useful, and we always invite your feedback at contact@japcc.org.

Vito Cracas
Colonel, ITA AF
Assistant Director, JAPCC

The Journal of the JAPCC welcomes unsolicited manuscripts.
Please email submissions to: **contact@japcc.org**

We encourage comments on the articles in order to promote discussion concerning Air and Space Power. Current and past JAPCC Journal issues can be downloaded from: **www.japcc.org/journals**

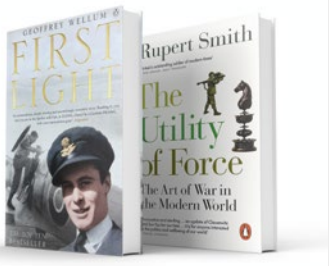
Follow us on Social Media

Table of Contents

Out of the Box

Inside the JAPCC

Book Reviews



Imprint

Transforming Joint Air & Space Power:
The Journal of the Joint Air Power Competence Centre (JAPCC)

Director
Air Marshal Johnny Stringer

Executive Director
Lieutenant General Thorsten Poschwatta

Assistant Director
Colonel Vito Cracas

Editor
Colonel Kevin Anderson

Assistant Editors
Major Tamás Oszlár, Major Lucas J. Stensberg

Production and Advertising Manager
Mr Simon J. Ingram

Editorial Review Team
Colonel Alexander Lorch, Colonel Matthew Hanson, Colonel William Barksdale, Colonel Patrick Parrish, Colonel Gianluca Chiriatti, Mr Adam T. Jux

Purpose
The JAPCC Journal aims to serve as a forum for the presentation and stimulation of innovative thinking about strategic, operational and tactical aspects of Joint Air and Space Power. These include capability development, concept and doctrine, techniques and procedures, interoperability, exercise and training, force structure and readiness, etc.

Cover Photo: A fifth-generation crewed fighter, accompanied by its uncrewed wingman, manoeuvres decisively into the future battlespace. The image highlights the fusion of crewed and uncrewed airpower, symbolizing Allied adaptability and innovation. Marking two decades of JAPCC's work with much more on the horizon, it captures both the progress made and the foreshadowing of what lies ahead for NATO joint air and space power.

20-Year Anniversary Reflection

Two Decades of Transforming Joint Air and Space Power

Introduction

The Joint Air Power Competence Centre (JAPCC) reached a significant milestone in 2025, marking 20 years since its establishment on 1 January 2005. As NATO's first accredited Centre of Excellence (COE), the JAPCC was formed to advocate and advance air power within the Alliance. For over two decades, the JAPCC has consistently pursued its vision to be 'NATO's catalyst for the improvement and transformation of Joint Air and Space Power, delivering effective solutions through independent thought and analysis'. This anniversary provides an opportune moment to recognize the JAPCC's role in advancing NATO's combat capability over the last two decades, while also acknowledging the changes and innovations required to meet future challenges.

In 2005, NATO found itself navigating a volatile post-Cold War security environment. The attacks of 9/11 had altered the trajectory of transatlantic defence priorities, highlighting gaps in operational readiness, doctrinal coherence, and strategic integration across domains. Operations in Afghanistan underscored the pressing need for agile, joint air capabilities that could seamlessly coordinate among allies and partners.

Recognizing this need, NATO endorsed the establishment of the JAPCC in Kalkar, Germany, with a mandate to offer independent expertise in air and space power. Designed as a multinational think tank working together with both Allied Command Operations (ACO) and Allied Command Transformation (ACT), JAPCC was tasked with bridging the gap between doctrine and execution. Its formation represented a

pivotal moment – a commitment to ensuring that NATO's air power strategy would be future-focused, collaborative, and continuously adaptive.

As a NATO accredited COE, JAPCC's work is organized around four pillars of work:

1. Concept Development and Experimentation (CD&E),
2. Education, Training, Exercises, and Evaluation (ETEE),
3. Doctrine Development and Standardization (DD&S),
4. Analysis and Lessons Learned (A&LL).

Concept Development and Experimentation

The JAPCC's role in CD&E is foundational to its mission of transforming joint air and space power. From its inception, the JAPCC has focused on developing and championing innovative visions, concepts, and solutions for Alliance challenges.

One consistent area of focus has been the space domain. Starting with the 'Space Operations Assessment for NATO' in 2008, JAPCC continuously advocated for NATO Space policy and doctrine. This persistent effort was instrumental in NATO's official recognition of space as an operational domain in December 2019, a significant evolution in Alliance thinking. This recognition led to a dedicated Space Branch within JAPCC in 2020, and recently, contributed to the establishment of a separate NATO Space COE in Toulouse, France. The JAPCC handed over the NATO Space Department Head responsibility to the Space COE in 2023, and both COEs continue to collaborate to advance joint air and space power.

The JAPCC has also consistently explored concepts for integrating capabilities across different military domains. This evolved from early work on a 'Network Enabled Environment' to the contemporary development of the 'NATO Joint All-Domain Operations (JADO)' project, initiated in 2021. JADO, now MDO, aims to transition NATO capabilities from merely coordinated joint activities to fully integrated actions across all domains. Besides integrating domains, the JAPCC has also led air platform integration, including the 2024 development of the Air-to-Air Refuelling (AAR) Compatibility Matrix, mapping out specific NATO Allied and Partner logistical relationships.

Adapting to evolving threats is another constant in JAPCC's CD&E. Early projects included support for Counter-Improvised Explosive Devices (C-IED) in Afghanistan, leading to numerous research studies and gap analyses. More recently, efforts have shifted to Counter-Unmanned Aerial Systems (C-UAS) studies and similar contributions addressing hybrid threats. Furthermore, the Centre has focused on enhancing base resilience, notably through the 'Resilient Basing Enhancement Workbook' (2022–2024), which aids nations in identifying potential vulnerabilities and mitigating shortfalls against evolving threats.

Looking to the future, JAPCC is actively developing concepts for Autonomous Collaborative Platforms (ACP) and Collaborative Combat Aircraft (CCA), recognizing their anticipated challenging role in future air superiority.

Education, Training, Exercises, and Evaluation

The ETEE pillar ensures NATO forces are prepared for advanced modern warfare against a peer adversary. Here, the JAPCC contributes by providing substantial support to NATO exercise design and execution, and by developing specialized training programmes and courses.

A hallmark of JAPCC's ETEE contribution is its role in shaping NATO's flagship exercises, including the 'Steadfast' and 'Ramstein Ambition' series. For two decades, JAPCC Subject Matter Experts (SMEs) have provided dynamic and realistic Opposing Forces (OPFOR) Air, Space, and Cyber, advancing NATO training against modern warfare threats.

In terms of specialized training, JAPCC led the development of Forward Air Controller-Airborne (FAC-A) simulation accreditation in 2009, allowing simulators to be used for qualification training, thereby reducing

costs and improving efficiency. In addition, JAPCC has been the Office of Primary Responsibility (OPR) for NATO Force Protection (FP) courses at the NATO School Oberammergau since 2009, continuously adapting the curriculum and developing an 'Advanced Force Protection Practitioners Course' in 2019. In 2025 JAPCC launched NATO's first C-UAS Fundamentals Course, teaching over 500 students in the first year alone.

Furthermore, JAPCC's direct support to the Baltic States' Air FP posture since 2015 has led to tangible improvements in regional security planning and resources. The Centre also maintains a valuable engagement with the European Safety & Security Professionals Network, bridging military, academic, and industrial perspectives to share best practices and influence future training curricula.

Doctrine Development and Standardization

The DD&S pillar is a less visible, but highly important, role within JAPCC. To ensure NATO's military guidance remains current and coherent, JAPCC SMEs work behind the scenes to draft, review, and refine numerous NATO documents and policies.

A cornerstone doctrine managed by JAPCC is Allied Joint Publication (AJP) 3.3, *Air & Space Operations Doctrine*. Since gaining custodianship in January 2013, JAPCC has continuously updated AJP-3.3 to reflect new capabilities and operational environments, ensuring it remains foundational guidance for Alliance air operations. Similarly, JAPCC has been deeply involved in Force Protection (FP) doctrine since 2010, authoring and holding custodianship for ATP-3.3.6, *NATO Force Protection Doctrine for Air Operations,* and AJP-3.14, *Allied Joint Doctrine for Force Protection*. This ensures FP principles evolve to address new threats.

Additionally, JAPCC plays a major role in standardizing air mobility, helicopter and fighter operations, and combat logistics. It published the *NATO Air-to-Air Refuelling (AAR) Flight Plan* in 2011 and has consistently updated and managed AAR doctrine and procedures. JAPCC also holds custodianship of ATP-49, *Use of Helicopters in Land Operations,* leading its restructuring and updating. JAPCC's support for Aircraft Cross-Servicing (ACS) efforts led to the promulgation of STANAG 3430 in 2020, enhancing interoperability. The Centre consistently contributes expertise to Alliance decision-making processes through active leadership and participation in numerous NATO committees, influencing Integrated Air and Missile Defence policy and overall NATO Security Policy.

'For over two decades, the JAPCC has consistently pursued its vision to be "NATO's catalyst for the improvement and transformation of Joint Air and Space Power, delivering effective solutions through independent thought and analysis".'

Analysis and Lessons Learned

Under the A&LL pillar, JAPCC provides independent thought, analysis, and solutions to address challenges and inform decision makers across the Alliance. This is achieved through a diverse programme of work comprising over a hundred projects, publications, and tasks per year.

Since 2008, the JAPCC has consistently hosted its annual Air and Space Power Conference, serving as a premier forum for stimulating debate, showcasing ideas, and gathering expert feedback on critical A&S issues. Conference themes have continually evolved, reflecting contemporary challenges; for instance, 2025's theme 'Disrupting Dominance,' highlights the increasing dilemmas between warfare capability (like exquisite sixth-gen fighters) and capacity (such as inexpensive drone swarms). In addition, the JAPCC Journal, published biannually, is our flagship publication, widely recognized for its thought-provoking articles from diverse experts, and serving as a vital communication channel for advocating NATO air and space power.

A historic commitment to NATO air and space power – at the ACT signing ceremony, senior military leaders laid the foundation for the establishment of the Joint Air Power Competence Centre in 2005. Based in Kalkar, Germany, the JAPCC continues to shape the future of NATO's joint air and space capabilities.

The JAPCC has demonstrated a strong commitment to self-assessment and strategic adaptation. An internal review in 2012 led to a comprehensive strategic transformation, re-aligning our focus towards more operationally and tactically oriented projects and enhancing engagement with NATO and Sponsoring Nations. This commitment to 'Relevance, Rigour, and Reputation' (principles adopted in 2010) ensures that our products remain current and impactful.

Collaborative knowledge sharing is a cornerstone of JAPCC's A&LL. Key to this are three major forums – the Annual JAPCC Conference, the Think Tank Forum (TTF), and the Joint Air and Space Power Network (JASPN) meeting, established in 2014. These gatherings bring together national, NATO, and EU organizations to share information, identify common interests, and prevent the duplication of effort.

Beyond these recurring events, JAPCC produces in-depth analyses and reports on specific challenges. Examples include the 2008 'Space Operations Assessment', the 2010 'UAS Concept of Employment', the 2010 'Air Basing Strategy', and the 2021 study on 'Big Data Management in ISR and New Technology Trends'. The JAPCC's analytical work directly informs NATO's Defence Planning Process (NDPP) by providing essential expertise on capability requirements and development.

Conclusion

In its 20 years of existence, the Joint Air Power Competence Centre has proven to be an indispensable asset to NATO and its Sponsoring Nations. Its consistent pursuit of independent thought and rigorous analysis, coupled with its adaptive approach to emerging challenges, has allowed it to effectively guide the transformation of joint air and space power. From pioneering air policy to investigating innovative technologies like ACP, and from developing foundational doctrine to providing exercise support, the JAPCC has continuously delivered relevant and high-quality solutions.

As the security environment grows more complex, the JAPCC's commitment to innovation, interoperability, and safeguarding Alliance interests remains paramount, ensuring that NATO's air and space power continues to be a credible, capable, and available cornerstone of deterrence and defence. The JAPCC's journey over the past two decades is a testament to its enduring relevance and its vital role as NATO's catalyst for transformation. ●

© US Air Force

The Combined Air & Space Operations Center (CAOC) at Al Udeid Air Base, Qatar.

Evolving C2 for Decisive Air Power

By Brigadier General Mehmet Serkan Dan,
TÜR Air Force, Deputy Chief of Staff Plans, AIRCOM

Introduction

NATO's ability to achieve decisive air effects hinges on command and control (C2) agility, yet contemporary threats increasingly challenge traditional C2 paradigms. While air superiority remains the cornerstone of success in modern conflict, sophisticated adversaries and high-tempo operations demand more than established principles; they necessitate a C2 evolution capable of maximizing effects, mitigating vulnerabilities, and driving the operational tempo against peer competitors.[1]

In this context, the traditional air power principles of centralized command and decentralized execution may no longer suffice for victory, given the threat environments of today and the future. The emergence of long-range ballistic missiles supported by advanced intelligence, surveillance, and reconnaissance (ISR) systems, stand-off munitions from low-observable aircraft, and offensive one-way unmanned aerial vehicles (UAVs) with precision strike capabilities underscores the need for new C2 approaches to sustain air operations against near-peer adversaries.[2] Consequently, this article argues that enhancing air power C2 survivability

NATO's E-3 AWACS leads a formation of fifth-generation F-35s, symbolizing the integration of surveillance, command, and strike capabilities. This synergy reflects the evolving C2 structure - centralized command coordinating with agile, forward-deployed forces through resilient, distributed control mechanisms.

and effectiveness requires adopting a distributed approach, strategically delegating execution authorities while retaining central strategic oversight.

The Enduring Imperative: Unity of Command

It remains essential that a sole air commander retains responsibility for commanding air forces and generating effects within the operational theatre. Without command integrity, air forces cannot be expected to gain and maintain air superiority. Fragmenting air forces without unity of command prevents the creation of desired effects, ineffectively dissipates resources, and ultimately hinders mission accomplishment. However, an approach based on appropriately distributing C2 authorities, while maintaining fidelity to central command, enables sustained operations in high-threat environments.[3]

An air force requires innovative design and active command, much like the human body relies on a functioning brain. However, the inherent vulnerability of C2 centres – due to imperfect air defences and their status as likely primary targets – necessitates the functional and geographical distribution of planning, coordination, and assessment processes, even while centralized command and approval authority remain vital for force management. Furthermore, when elements operate with initiative in dynamic environments, guided by the commander's intent, they effectively translate plans into action on the ground. In short, centralized command, distributed control, and decentralized execution form the cornerstones of the modern air C2 approach.[4]

Agility for Resilience

The Ukrainian Armed Forces' ability to sustain prolonged resistance against Russian forces, stems in part from an operational dynamism that seeks to complicate and disrupt the enemy targeting cycle. Specifically, the Agile Combat Employment (ACE) approach – whereby fighter jets and surface-based air and missile systems remain mobile rather than fixed – has been a notable contributing factor to their survivability, alongside other critical operational adaptations such as carefully managing their exposure within contested airspace. Successfully continuing operations from dispersed airfields has enabled Ukrainian air forces to remain viable and defend their nation.

While individual dispersed elements under ACE may face increased risks of intermittent connectivity, integrating the ACE concept into a distributed C2 framework is intended to enhance the resilience of overall command effectiveness. This approach mitigates the risk of a catastrophic single-point failure in the C2 system, even if some components temporarily operate with degraded communication. One example of ACE methodology is

Distributed control empowers subordinate nodes with delegated authorities, supporting the commander's intent and sustaining operations.

the use of concealment and deception. Supporting movement cycles with active and passive deception methods is a key aspect of warfare and has been instrumental to numerous historical victories. Achieving a high level of agility and resilience, however, relies not only on physical dispersal and movement, but also on an underlying C2 structure that empowers timely decision-making closer to the point of execution. Realizing such empowerment, in turn, necessitates distributing control functions, built upon a foundation of mutual trust and shared understanding of strategic objectives.

Furthermore, it must be acknowledged that for complex Composite Air Operations (COMAOs), 'shared understanding' alone is insufficient for precise synchronization. The successful aggregation and coordination of diverse force elements from dispersed locations under ACE fundamentally relies on robust, resilient, and sufficiently redundant communication and information systems (CIS) capabilities, as outlined later, to facilitate essential data exchange and command direction, even if such communication is intermittent or constrained. The Ukrainian experience, often involving smaller, more agile packages, offers lessons in survivability, but scaling to large NATO COMAOs under distributed C2 will require thoroughly developed tactics, techniques, and procedures (TTPs) and technological enablers for coordination beyond just strategic alignment.

Executing Commander's Intent Through Distributed Control

Functionally, distributed control involves delegating specific authorities to relevant components according to protocols and orders to execute the commander's intent, retain initiative, and maintain operational synchronization. This distributed structure, typically involving delegation at the operational and tactical levels, allows subordinate units to perform specific Combined Forces Air Component Command (CFACC) functions proactively, based on the commander's course of action, or reactively in situations like communication loss. Operational intensity, unique geography, and time constraints may define the scope of delegated responsibility.

The operational level of warfare involves planning and executing major operations using military art to achieve strategic objectives. The CFACC and subordinate Air

Operations Centres (AOCs) are the primary elements managing, coordinating, and synchronizing air power activities. Achieving the desired transformation involves distinguishing between C2 functions: while strategic tasks such as deployment plans, contingency plans, sustainment activities, and long-term planning remain centralized, tasks such as the production of Air Tasking Orders (ATOs), focused on the near-term, should be delegated to subordinate echelons, accommodating varying command preferences as needed.[5]

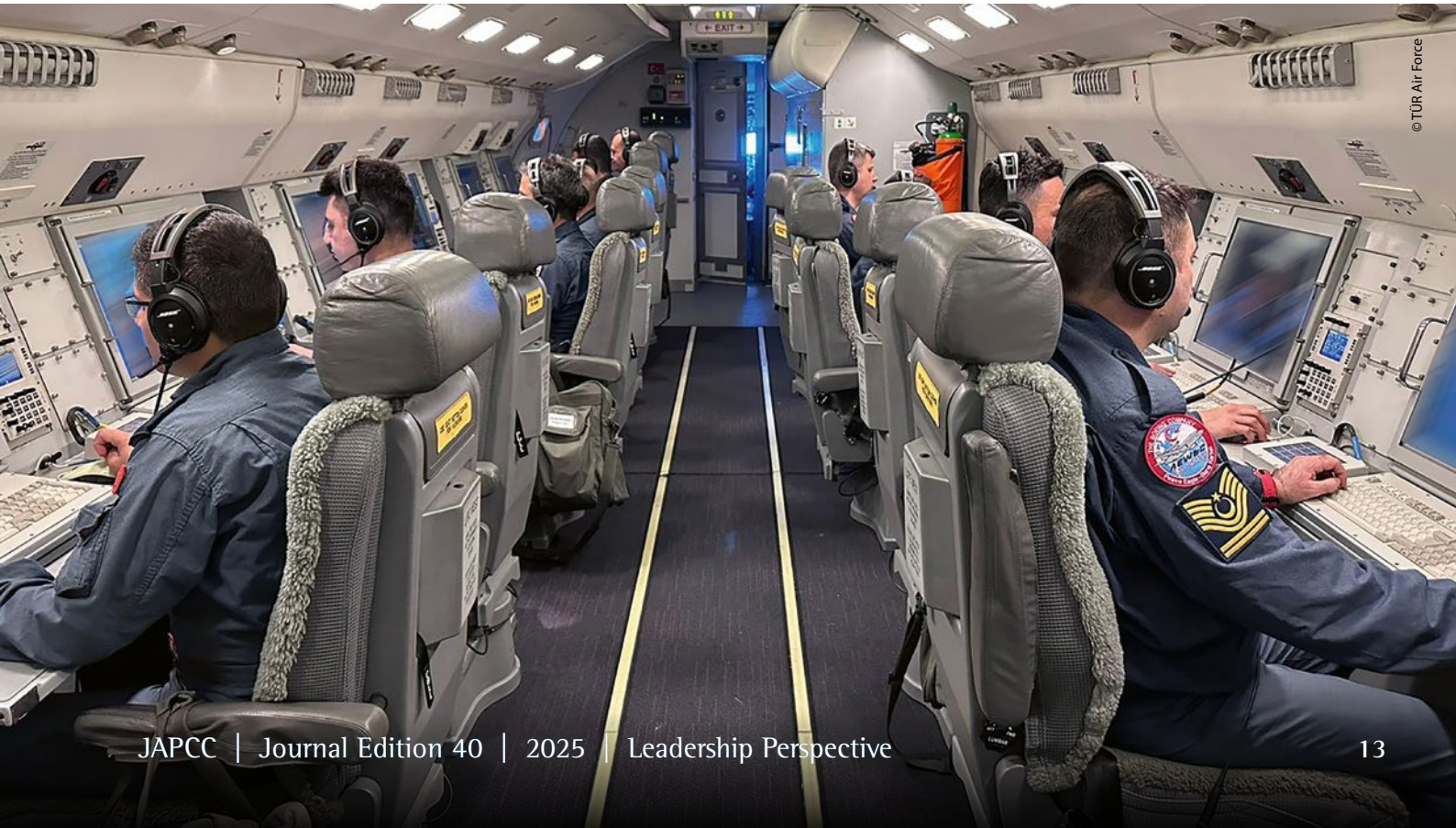
Moreover, since complete protection from air defence systems is unrealistic due to the ongoing technological race, distributing these elements geographically and functionally provides optimal sustainability. Dispersing operations centre personnel to suitable locations in depth and along different axes, rather than concentrating them in a single centre, mitigates the vulnerability of potential enemy attacks restricting or eliminating C2 functions. In this distribution model, dispersed personnel and functions serve as functional backups to the CFACC; if primary capabilities are attacked, these redundancies ensure C2 cycle continuity.[6]

For example, during extensive operations against a near-peer adversary, centralized command can be maintained while delegating authorities to subordinate command centres based on their geographical expertise, experience, and capabilities. A robust CIS infrastructure that can support the transfer of functional responsibilities enhances flexibility. Critically, the operations centres receiving delegated control must possess the necessary technical capability, operational experience, and personnel quality and quantity to effectively manage the cycle.

'The key criterion is whether distributing the function enhances tempo, resilience, and lethality without compromising overall operational coherence or risking fratricide.'

At the tactical execution level, distributed control is currently delegated to an Air Battle Manager (ABM) located in a ground or airborne C2 node, or it may involve a fighter pilot serving as the Mission Commander or package leader. However, the concept of distributed control discussed in this article moves beyond traditional decentralized execution by formally delegating specific C2

Airborne C2 nodes support dynamic decision-making and ensure operational synchronization.



Forging air superiority through distributed command: A formation of NATO F-16 fighters exemplifies the agility and cohesion required for modern air operations.

authorities and responsibilities, typically resident within a primary AOC, to designated subordinate echelons or geographically dispersed nodes. This could mean one subordinate C2 node is empowered with dynamic targeting approval for a specific region based on pre-agreed authorities, while another assumes lead responsibility for integrated air and missile defence (IAMD) in its sector if the primary AOC is compromised. To achieve distributed control, nodes must operate with a common operational picture, shared C2 processes, and clear hand-over/take-over protocols for these delegated functions, ensuring that control itself, not merely the execution of tasks, is resilient and adaptable.

Awaiting Challenges: Towards a Distributed Future

Transitioning to a truly effective model of centralized command, distributed control, and decentralized execution presents significant, though surmountable, challenges that require deliberate attention. While the principle is sound, its practical application demands careful consideration of which functions are best suited for delegation away from the central CFACC.

Functions potentially suitable for delegation could include aspects of near-term operational planning (like ATO production), dynamic targeting authority, certain airspace control functions in specific sectors, localized IAMD engagement decisions, and potentially, elements of tactical-level ISR tasking and fusion. The key criterion is whether distributing the function enhances tempo, resilience, and lethality without compromising overall operational coherence or risking fratricide.

However, such distribution inherently introduces follow-on challenges. Maintaining synchronization and deconfliction across geographically or functionally dispersed control nodes becomes more complex. Ensuring every echelon understands and adheres to the overarching commander's intent, is therefore paramount, and leadership initiative must be encouraged under degraded communication conditions. There is an inherent risk that decentralized execution, if not bounded adequately by clear rules of engagement and intent, could diverge from the central plan, leading to suboptimal outcomes or unintended consequences. Furthermore, verifying the capabilities and readiness of subordinate echelons to assume these delegated responsibilities requires rigorous assessment.

Overcoming these hurdles necessitates a concerted effort. It demands the careful development of a robust doctrine that clearly outlines authorities, responsibilities, and limitations within a distributed C2 framework, with an emphasis on pre-negotiated authorities

and robust data synchronization strategies. New TTPs must be meticulously crafted and validated. Perhaps most importantly, these concepts cannot merely exist on paper; they require extensive rehearsal through demanding exercises and wargames. These events must realistically simulate the high-tempo, contested, and communication-degraded environments where distributed control is most needed, allowing forces to identify friction points, refine procedures, build trust, and validate the model's effectiveness before it is relied upon in actual conflict.

Pathway to Implementation

Given the established need for conceptual transformation in air power management, the essential question is, 'What should we do?' Effecting these changes requires a rapid, practical integration process, and the DOTMLPFI (Doctrine-Organization-Training-Materiel-Leadership-Personnel-Facilities-Interoperability) framework provides a structure to identify the necessary actions, which are grouped logically below:

Doctrine:

- Define, document, train, test, and refine TTPs with a 'train as you fight' mentality.
- Establish necessary information-sharing procedures and permissions between elements in peacetime.
- Ensure doctrine supports the ability to execute and synchronize Multi-Domain Operations (MDO), incorporating cyber and space effects within the distributed structure.

Organization:

- Structure forces and command relationships to support distributed control, ensuring designated subordinate centres are appropriately resourced and empowered.
- Delegate responsibilities in accordance with regional and functional expertise.
- Maintain the organizational capacity for MDO synchronization even within a distributed C2 model.

Training:

- Implement rigorous training programmes focused on developing skills needed for decentralized execution, including initiative, understanding the commander's intent, and operating under degraded conditions.
- Utilize demanding exercises and wargames to test and refine distributed C2 concepts and build trust.

Materiel:

- Ensure robust, resilient, and sufficiently redundant CIS capabilities; explore and leverage cloud-based systems and low-orbit satellite communications.
- Pursue automation and, where feasible, artificial intelligence applications to enhance C2 functions and alleviate personnel demands.
- Enhance IAMD capabilities across all layers to protect C2 nodes and forces.

Leadership:

- Cultivate leadership that fosters mutual trust and encourages appropriate initiative within the commander's intent.
- Ensure leaders at all levels are trained to communicate and understand the overarching mission goals and intent.

Personnel:

- Develop well-trained, adaptable, critically-thinking, and 'warrior-spirited' air personnel capable of making sound decisions under pressure and with delegated authority.
- Identify manpower requirements for distributed operations and ensure personnel possess high situational awareness.

Facilities:

- Prepare and potentially harden designated primary and alternate/dispersed C2 facilities, considering geographic distribution and specific roles (e.g. subordinate AOCs).
- Select facility locations considering physical infrastructure, access to expertise, and regional knowledge.

Interoperability:

- Develop and regularly exercise standardized NATO procedures for distributed C2 scenarios.
- Invest in C2 architectures designed for interoperability within NATO and with designated mission partners. Utilize open standards and flexible interfaces.

- Establish and enforce common NATO data standards, communication protocols, and interoperable C2 system interfaces.

Implementing this transformation requires a fundamental shift in mindset alongside these tangible actions. This list is, of course, not exhaustive, and leaders must proactively examine their own organizations for distribution and delegation opportunities.

Conclusion

Change is constant, yet transforming established ideas and practices often meets resistance. Air power, a decisive factor since World War II, owes its success to intellectual leadership and adaptability. NATO airspace, territory, and territorial waters, defended through active deterrence for over 75 years, require continued protection achieved by accurately analysing operational risks and developing counterstrategies. As underscored in the title, achieving decisive power in future conflicts hinges on evolving our C2 structures to match the speed, complexity, and lethality of the modern battlespace. The proposed model of centralized command, distributed control, and decentralized execution directly contributes to this decisiveness by enhancing resilience against attacks on C2 nodes, increasing operational tempo through empowered subordinate echelons, and fostering the initiative needed to outpace adversary decision cycles.

Demonstrating our superiority in how we wage war, particularly through evolved C2, is a credible way to ensure deterrence and collective defence – NATO's core tasks. A well-functioning distributed control process is an effective deterrent when perceived by adversaries and guarantees functional C2 in high-intensity air operations. However, this evolution must be proactively accomplished. Implementing and exercising the concepts discussed in this article during peacetime is, therefore, critical and should proceed without delay. ●

1. Bronk, J., The Air Power Journal, [website], 2021, https://theairpowerjournal.com/decentralized-c2-air-operations-battle-management-mission-command/, (accessed 17 January 2025).
2. Ibid.
3. Mulgund, S., Wild Blue Yonder, [website], 2021, https://www.airuniversity.af.edu/Wild-Blue-Yonder/Articles/Article-Display/Article/2575321/evolving-the-command-and-control-of-airpower/ (accessed 18 January 2025).
4. Ibid.
5. Harvey, S, A., 'The Levels of War as Levels of Analysis', Military Review, November-December, 2021, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2021/, (accessed 19 January 2025).
6. Coleman, F., Mitchell Institute, [website], 2023, https://www.mitchellaerospacepower.org/app/uploads/2023/01/MI_Forum_50-C2-Distributed-Control-FINAL.pdf, (accessed 19 January 2025).

ABOUT THE AUTHOR

Brigadier General Mehmet Serkan DAN

TÜR Air Force, AIRCOM

Brigadier General Mehmet Serkan DAN graduated from TÜR Air Force Academy in 1996. As a fighter pilot and weapons and tactics instructor, he served at numerous positions and various operational missions with more than 4,000 flight hours in F-4, E-7, and F-16s. After graduating from Air Force Institute at 2021 and commanding TÜR AWACS Group, promoted to Brigadier General and assigned as Commander of 10th Main Jet Base-Incirlik. He has been assigned to NATO Allied Air Command, Ramstein, Germany, as DCOS Plans since 4 September 2023.

AALTO

UNLOCKING STRATOSPACE

Operating at 60,000+ feet

AALTO Zephyr is a world-record-breaking High Altitude Platform Station (HAPS) that can deliver resilient Earth observation and direct-to-device capabilities from the stratosphere, for days, weeks and months at a time.

FIND OUT MORE:
aaltohaps.com

Global Combat Air Programme

Mutual Defence Going Global

Colonel Maurizio De Guida, ITA Air Force
Group Captain Bill Sanders, UK Royal Air Force
Colonel Taro Murao, JPN Air Self-Defense Force

Introduction

The world is navigating a moment in history where geopolitical context has brought the return of nation-state level conflict, previously considered unthinkable by many. It reminds us that security should not be taken for granted as we witness the beginning of a new era of worldwide international competition and disorder. National security and sovereignty have evolved into more complex and interconnected concepts that extend far beyond state borders. In today's globalized world, we are all inextricably linked to events, developments, and actors, no matter how geographically separated, rendering the strategy of isolation a mere illusion. Even if you live in the luxury and security of a penthouse, when the ground floor is on fire it is only a matter of time that you will be in trouble as well. Air power can exploit its speed, height, and reach to be the firefighters going FAST, going FAR, unimpeded and with short notice.

Current conflicts have reminded us that control of the air – a core competency of our tri-lateral and allied air forces – is still vital for national security because it enables the effectiveness of all other domains, perhaps more than ever before in history, especially considering increasing disparities in force size. Investing in the ability to control the air domain protects us from the alternatives, such as attritional warfare, where the cost in blood and gold is far greater than the cost required to control the air. Therefore, when thinking of future combat air capabilities through a global mindset, there are direct implications for certain characteristics and requirements such as range, logistics, and operational agility (high interoperability, low footprint, fast updates, and capabilities to adapt to new scenarios).

New and evolving threats and counters drive a mindset-shift in the requirements of traditional capabilities in the same way that drones have challenged the whole concept of armoured vehicles. Strategic offset strategies like Anti-Access/Area Denial (A2/AD) and an increasingly layered and contested zone have taken air power 'back to the future' calling for 'Survivability 2.0'. Just as with the maritime, land, and space domains, Control of the Air is now more diverse, high-stakes, and difficult than ever. At the same time, developments in cyberspace and space are altering long-standing assumptions and perspectives in all the traditional domains. With modern threats and in our technical environment,

there is even less time to prepare or update existing tools before the point of crisis.

These factors are why the development of future combat air systems is such a high priority for so many countries. Rooted in the European and Indo-Pacific regions, Italy, Japan, and the UK are leveraging their multiple commonalities – their operational journey with fifth generation aircraft, a proud and thriving aerospace and engineering industry, and a long, strong aviation history. Taking together all these common foundations, they bridge geographic and language barriers resulting in a tri-lateral arrangement that has the means, the understanding, the need, and the desire to commit to the next generation of combat air systems. The Global Combat Air Programme (GCAP) team has the responsibility to communicate our plan to our alliance partners to foster understanding and confidence in our choices and strategy. Also, because – sooner or later – we may employ several different systems alongside one another in the same formations and in the same challenging theatres. What follows is a discussion about the philosophy behind GCAP's development; by sharing these goals, we hope to increase the understanding of the program by NATO and our other allied partners.

Why We Declare 'Sixth-Gen' Up Front:

Military aviation technology is on the cusp of another significant leap forward in capability. In the last hundred years, the evolution of air systems has not followed a linear path, but rather it has been marked by sudden leaps and moments of strong discontinuity despite its overall rapid progression. Innovative technologies have enabled those leaps which in turn changed the rules of air warfare, such as radars, precision weapons, integrated avionics, and low observability. Those technologies have revolutionized doctrines, concepts of employment, and tactics. They have shaped the way effects are generated in and from the sky. As the air domain has established itself over the past century, it has been at the centre of key developments across domains from the Blitzkrieg through the second offset of the Gulf Wars.

Conditions are primed for another leap that will result in a capability level that justifies the naming of a new generation of fighter aircraft. Multiple diverse, but related, technologies are reaching maturity or rapidly developing in a disruptive way – driven by both commercial pressures and conflict – which will result in GCAP being more than 'just another fast jet'. GCAP is more than new stealth technologies, new effectors, the capability to coordinate collaborative combat aircraft

In December 2022, the Governments of Italy, Japan, and the UK announced the launch of the Global Combat Air Programme to develop a next-generation fighter.

(CCAs), or doing tasks with more autonomy than ever before. Instead, GCAP is a new paradigm of integration amongst platforms, systems, and components across all domains, including space and cyber that provide GCAP access to a whole range of 'new wingmen.'

This article details 'what' we need; however, more interesting should be 'how' we deliver it.

Capability Management from F-35 Users' Perspective

Italy, Japan, and the UK share common experiences and understandings through their experience with the F-35 programme. As F-35 users, GCAP nations are committed to developing a collaborative, complementary platform – not a competitor nor replacement of the F-35. GCAP has already digitally flown extensively in challenging virtual environments to assess performance and refine requirements among the competing interests and priorities. In this context, GCAP is deliberately positioned to be a complementary asset within the broader air power portfolio, enhancing – not replacing – the capabilities of the F-35.

To complement existing air power platforms, the main challenge is not only having the right set of capabilities, but rather in integrating new systems like GCAP into multinational operations from day-one, addressing interoperability with existing systems, and ensuring cultural shifts to train airmen to navigate the increasing complexity of today and tomorrow's operational environments.

Connect or Lose

Since Harold Brown's second offset in the 1970s, we and the other allied nations have sought to use technological means to offset an adversary's superior force size. The threat's numerical advantage remains, but the last 25 years have seen our technological advantage eroded and even overtaken in some areas. It is increasingly clear that the allied nations' advantage now resides in the information advantage, operational tempo and capability adaptability; all enabled by the combination of technology, training, tactics, and command and control (C2). Against a numerically superior threat employing increasingly peer technical capability, the only means to achieve the effectiveness required is for each of our fighting elements to be greater than the sum of their parts. In the air domain, the F-35 has been extraordinarily successful at this at a formation level, highlighting both the fundamental importance and the challenges of connectivity in the contested area. As A2/AD doctrine and technology increases the size of contested regions ever more, these are becoming even more congested. We are faced with conflicting challenges to our control of the air and freedom of manoeuvre:

- Our tempo and flexibility advantage are dependent on connectivity and transmissions.
- Those emissions are in tension with survivability in a contested region.
- Contested regions are expanding and becoming more congested.
- A greater proportion of our assets and capability must be capable of operating in the expanded contested regions.

It is becoming clear to all, including the threat, that connectivity is fundamental to our capability advantage. We must stay connected, or we lose. GCAP is being developed under this clear imperative and is actively incorporating lessons from past capability programmes to ensure it is a net contributor to connectivity across all domains.

GCAP's Contribution to Conventional Deterrence

Like all military programmes, GCAP has a responsibility to justify its cost and demonstrate value for money. The war in Ukraine has reminded everyone that conflict is always more expensive than deterrence; however, deterrence is not an argument for unconstrained cost because it is vital that nations' capability programmes identify the most efficient and cost-effective means to achieve the desired capability. Additionally, combat air systems are

GCAP is being developed from the outset as the core of a system-of-systems, providing the processing, sensors, and connectivity to enable high volume CCA.

good value for money because they provide adaptable, multi-use capability at every level, from peace to full-scale conflicts. Since development of that combat air capability advantage is a highly challenging and expensive endeavour, collaboration between like-minded and well-matched allies is the solution. Italy, the UK, and Japan are pooling our resources and sharing the costs and the burden to develop GCAP.

GCAP's freedom of manoeuvre is enabled by its evolved survivability, advanced sensing, expanded combat radius, and kinetic- and non-kinetic payloads. The combination of survivability, range, and payload allow GCAP to hold adversaries' logistical and supply lines, infrastructure, industrial and manufacturing bases, and C2 components at risk. GCAP freedom of manoeuvre and range forces the adversary to dilute its defences over a much wider area which increases other allied assets' freedom of manoeuvre, thus enabling the contribution of less capable platforms.

GCAP will provide commanders fully scalable options from non-kinetic to significant volumes of high-yield, wide-area, or long-range kinetic effectors. Few assets offer the level of deterrence and freedom of manoeuvre that a credible, long-range, persistent, and survivable platform can–and those that do are rare. The conventional deterrence and freedom of maneuver provided by GCAP will benefit our nations and our allies. Securing that deterrence capability will always be cheaper than the conflict it prevents. It represents a cost-effective and integrated solution for the three nations and all our alliance partners.

GCAP's Approach to Payload: Not Just Weapons or Sensing

GCAP's role as a connectivity node capable of operating deep in a contested region explains why we have expanded our approach to payloads and the resulting benefits. Payload is the fundamental purpose and priority of the GCAP system:

© WolfWork JAPAN/Shutterstock.com

GCAP is embracing innovative methodologies for faster, cost-effective development and adaptation.

- Kinetic effectors are the first and obvious component of GCAP's payload. We are making every effort to maximize the new platform's flexibility and relevance. This involves applying adaptability lessons from the B-52, which has a long history as a 'payload reinvention platform,' and incorporating lessons on survivable combat air payload bays from the F-22 and F-35. Kinetic payload and magazine depth (at a platform and formation level) are being driven by the adversaries' saturation tactics, hardening, dispersal, contested electromagnetic environment (EME), and expanding range of A2/AD. These same factors are driving effector size and numbers, which in turn puts pressure on the bay sizes of aerial vehicles. Low-cost asymmetric threats are driving consideration of cost-per-kill and stockpile sustainability which in turn puts pressure on payload bay adaptability. Addressing all this is core for GCAP's concept and design.
- Non-kinetic effectors are the second, and increasingly normalized, component of the payload, providing the combat air form factor with previously unprecedented capabilities. But non-kinetic capabilities drive array size, to which power generation challenges must be solved.
- As the third component of the GCAP payload, the sensor suite provides crucial situational awareness and high-fidelity insights. To enable freedom of maneuver, sensor reach is vital, even with impressive survivability. However, sensor range remains proportional to size and power, creating a challenge for the platform's overall size, weight, and power (SWAP) limitations.
- Connectivity is a critical fourth component of the GCAP concept. It serves two purposes: first, it allows GCAP to exploit other capabilities, ensuring it contributes as much to situational awareness and tempo as it consumes. Second, it creates a survivable network node deep within contested environments, enabling less capable, lower-cost, or expendable parts of the overall system to participate.
- Finally, computing represents the fifth component of the GCAP payload, becoming increasingly essential

as the high-low mix concept is leveraged. It enables operations within contested environments by integrating with local and survivable networks to deliver the computational support, functional capabilities, and operational tempo required across platforms to achieve mission success.

GCAP is aiming to balance the five components of payload with its survivability and range to provide the freedom of manoeuvre to deliver and sustain the payload where it is needed.

Effects Reach

GCAP integrates payload, range, and survivability to establish what the programme defines as 'Effects Reach'. Survivability constrains combat radius, while the range of payloads – whether sensors or effectors – is limited by survivability factors (such as external stores or emissions) or by SWAP constraints (including bay size, radar cross-section, and aerodynamic drag). The interplay between combat radius and the range of sensors and effectors determines GCAP's overall 'Effects Reach'. This concept serves as a framework for assessing GCAP's freedom of manoeuvre and ability to hold targets at risk that other platforms cannot. This insight has guided critical design and capability choices during the development phase to ensure the platform achieves its intended effectiveness and capability.

Crewed vs Uncrewed: The Role of the Quarterback

GCAP is being developed from the outset as a formation-capable, system-integrated, and system-of-systems platform. While it must retain the ability to operate independently in high-threat or contested EME, its design prioritizes leadership, coordination, and integration with other platforms–whether from other GCAP platforms, crewed systems, or assets within human-machine teams. The 'quarterback' metaphor, increasingly associated with 'sixth-gen' crewed platforms, aptly captures this role. A quarterback platform must be survivable enough to endure threats, capable of independently delivering decisive effects, but most effective when adapting to and orchestrating the actions of other assets in real time.

Even when isolated within the contested region, GCAP will remain capable of enacting the strategic intent tactically but with the intelligence to dynamically adapt the plan in response to adversary behaviour. This metaphor encapsulates several emerging requirements for 'sixth-gen' offensive core platforms: limited reliance on reachback connectivity once deployed; integration with less capable or expendable systems; technology to enable the networks and processing to support tempo and adaptability; concentrated C2 authority; and the flexibility to trade traditional attributes like speed for enhanced capabilities. Although developing such a core platform is complex and resource-intensive, it is essential for realizing the 'greater than the sum of its parts' operational concept. This approach is critical to achieving the necessary operational tempo, effectiveness, and enablement of CCA operations by providing resilient communications, sensing, computing, and C2 capabilities within contested environments.

Conclusion

The trilateral partnership among Italy, the UK, and Japan is advancing GCAP development through a systemic and integrated approach from the outset. This strategy aims to prevent a future scenario – 10 to 15 years from now – where a fragmented fleet of fourth-, fifth-, and sixth-generation fighters operates with limited interoperability, constrained by divergent safety standards, security regulations, and industry priorities. The risks associated with such fragmentation are too significant for any single nation to manage independently, including the most capable states. In today's strategic environment, fragmentation is no longer a viable option. Failure to act cohesively now would necessitate even greater effort and resources to rectify the consequences later. For these reasons, and in alignment with the opening remarks of this article, we welcome this opportunity to share our perspectives, challenge the traditional definitions and roles of combat air, and lay the groundwork for robust cooperation among NATO Allies and Partners. ●

ABOUT THE AUTHORS

Colonel Maurizio De Guida

ITA Air Force

Col Maurizio De Guida is currently assigned to the GCAP Government Agency (Reading, UK), as Requirements Management and Operational Factors branch lead. He joined the Italian Air Force in 1998. After Pilot Training in Sheppard AFB (ENJJPT) he was assigned to AM-X, progressing to Qualified Weapons and Tactics Instructor. He has been selected for an exchange with the USAF, on A-10C. He then transitioned to F-35A, serving as Squadron Commander and leading to Initial Operational Capability (IOC) the first F-35 OCONUS Operational Unit. With over 3,200 hours, including 600 in real operations, he joined the Air Staff Policy and Plans department, focusing on Air Force Capabilities Requirements and then Chief of Future Combat Air System–Planning Office. He holds a degree in Political Science, a master's degree in Leadership and Strategic Analysis and attended NATO Defence College Senior Course.

Group Captain Bill Sanders

UK Royal Air Force

Group Captain Bill Sanders leads the UK's Requirements and Concepting team contribution to the tri-lateral Global Combat Air Programme (GCAP). He has served as a pilot in the Royal Air Force for 30 years; with an operational career that began on the Tornado F3 Air Defence Variant, before moving to the Typhoon FGR4 and in the process accumulating over 2,000 flight hours across the two types. He is a Qualified Weapons Instructor with a Test & Evaluation and capability acquisition background–specializing in sensors, data-links, and weapons integration. For the last 10 years he has worked exclusively in Combat Air capability acquisition and management in large multi-national programmes.

Colonel Taro Murao

JPN Air Self-Defense Force

Col Taro Murao currently serves as the Flight Group Commander of the 3rd Air Wing (Misawa Air Base) which operates F-35As. He was assigned as Chief of the GCAP Office, Defense Plans/Policies and Programs Division, Air Staff Office, JMOD. During this assignment he coordinated JASDF operational requirements with Italy and UK within GCAP Programme. Throughout his career he has over 2,000 flight hours, mainly on the F-15J. He previously was commander of the 204th Fighter Squadron (Naha Air Base), Okinawa. He earned his wing through SUPT in the US Air Force and he is a graduate of the US Air War College, the Republic of Korea Joint Forces Military University, and Osaka University.

Extending NATO's Safety Net: An HH-60G Pave Hawk of the 56th Rescue Squadron (RQS), with elite Pararescuemen from the 57th RQS, based at Aviano AB, Italy. These dedicated teams provide critical combat search and rescue capabilities, ensuring 'That Others May Live' during Alliance operations.

No One Left Behind: Rebuilding NATO's Rescue Mission

Why Revitalizing Joint Personnel Recovery Is Mission-Critical for the Alliance

By Major Brennan Gallagher, US Air Force, HQ AIRCOM

Introduction

In Operation Allied Force, a moment of high-stakes survival unfolded that would shape NATO's perspective of joint personnel recovery (JPR). On 2 May 1999, then-Lieutenant Colonel David Goldfein was flying his F-16 over hostile territory when a Serbian surface-to-air missile struck, compelling him to eject behind enemy lines. Isolated and vulnerable, Goldfein transmitted his famous plea, 'Start finding me, boys.'[1] What followed was a tense and methodically coordinated rescue mission – Operation Allied Force's only successful conventional combat search and rescue (CSAR) mission. This singular event underscored the profound importance of JPR to the Alliance.

Today's operational landscape differs from the challenges faced in 1999 Kosovo. Modern battlespaces are now dominated by sophisticated threat environments and advanced long-range missile systems. Over the

French Special Forces conduct a Survival, Evasion, Resistance, and Escape (SERE) exercise, simulating the recovery of a non-ambulatory isolated personnel. Standardized SERE training is an integral part of the NATO JPR interoperability.

same period, NATO's necessary dedication to counter-insurgency (COIN) operations, compounded by evolving strategic priorities and resource pressures, has inadvertently eroded institutional knowledge of JPR in peer conflicts and diminished its overall emphasis. Consequently, if a pilot like Lieutenant Colonel Goldfein were isolated today, JPR forces would face immense challenges. The pervasive nature of advanced sensors, formidable integrated air defence systems, and contested airspace now demands a renewed and robust approach to NATO's personnel rescue mission.

This article energizes the strategic commitment – moral, mental, and financial – to JPR, not specific platforms. It argues that NATO Headquarters, Supreme Headquarters Allied Powers Europe (SHAPE), Joint Force Commands (JFCs), Theatre Component Commands, and member nations must significantly increase focus, funding, and dedicated personnel to enhance Alliance JPR capabilities. This investment is crucial for the moral duty to protect personnel, combat power reconstitution, and Alliance cohesion. To achieve this, NATO must reaffirm the core purpose of JPR investment, establish an integrated, institutional Joint Personnel Recovery Centre (JPRC), and revitalize isolated personnel (ISOP) recovery capability through investment, education, training, and exercises.

Organizational Gaps

Since 1999, several factors have eroded NATO's JPR organizational structure and readiness. Adversary technological advances, a lengthy Afghanistan focus, and competing priorities reduced emphasis on JPR for high-intensity conflict. Many tactics, techniques, and procedures and equipment were designed for Middle East conflicts involving air supremacy against less advanced foes, leaving doctrine ill-suited for peer or near-peer threats. NATO's many other priorities also demanded substantial resources.[2] These constraints require careful rebalancing to ensure foundational, no-fail missions like JPR are not compromised.

In short, cumulative changes have weakened NATO's JPR organizational structure and overall readiness. The

Alliance must urgently train and stress its JPR C2 networks and recovery forces under anti-access/area denial (A2/AD) conditions, carefully balancing operational risk. JPR forces need exposure to these environments before an Article 5 scenario. NATO members must also procure interoperable JPR assets and technologies to ensure national efforts contribute effectively to collective capability. Without interoperability, the full potential of combined efforts is lost. Critically, NATO must establish a persistent, resourced JPR structure and conduct realistic exercises to ensure future isolated personnel like Goldfein return with honour.

Operational Guidance

JPR is a complex operation requiring joint, inter-allied, inter-partner, and often cross-government cooperation. Sustained multinational collaboration is essential to synchronize Alliance JPR efforts. In 2022, the Multinational Capability Development Campaign (MCDC), led by the US Joint Staff J-7, published 'JPR 2040: A Global Perspective,' highlighting strategic observations within JPR.[3] The study identified themes including building a comprehensive PR mindset, expanding scope to new threats and environments, and accelerating technology adoption.[4] The MCDC aimed to identify critical gaps in policy, doctrine, education, training, exercises, and evaluations facing future JPR challenges.

While the MCDC report effectively outlines the organizational gaps and operational challenges facing today's JPR forces, it was intended as a diagnostic, not a prescriptive, document. This article builds on that foundation by proposing concrete solutions. NATO JPR stakeholders must act on these challenges proactively, before a crisis exposes shortcomings. The MCDC concluded that without adaptation, education, and realistic training, JPR forces will be unprepared for future conflicts.[5]

A Marine ignites a smoke flare at MCB Hawaii, emphasizing the need for standardized, rigorous JPR training across NATO forces to ensure readiness, interoperability, and mission success in complex, high-threat environments.

© Marine Corps Cpl. Matthew Kirk

The Moral Imperative

The core argument for robust JPR capabilities is the moral imperative – an ethical contract and unwavering commitment between NATO leaders and personnel placed in harm's way. Since ISOP accept significant risk for NATO goals, the JPRC, subordinate Personnel Recovery Coordination Cells, and tasked forces are responsible for their recovery. SHAPE, NATO's highest strategic military headquarters, is responsible for safeguarding warfighters. The warrior ethos and commitment to 'leave no one behind' are fundamental military values shared across the Alliance.[6]

Failing to invest adequately in personnel recovery risks severely undermining service members' trust in NATO leadership. Such failure sends a chilling message about how individuals are valued, which can harm recruitment, retention, and morale. Additionally, the psychological impact on deployed forces – aware of weak recovery capabilities – can reduce operational boldness and risk acceptance. Conversely, a strong JPR system signals firm commitment, boosting the psychological resilience of every soldier, sailor, and airman.

SACEUR's vast area demands more rescue forces than any single entity can provide. A robust, Alliance-wide personnel recovery system – featuring effective C2 networks, rapidly deployable quick reaction forces (QRFs), and well-rehearsed CONOPS – reassures NATO personnel and their families they will not be abandoned.[7] Personnel must be confident that capable JPR forces, with coherent C2, will exhaust every effort to bring them home.

Combat Reconstitution

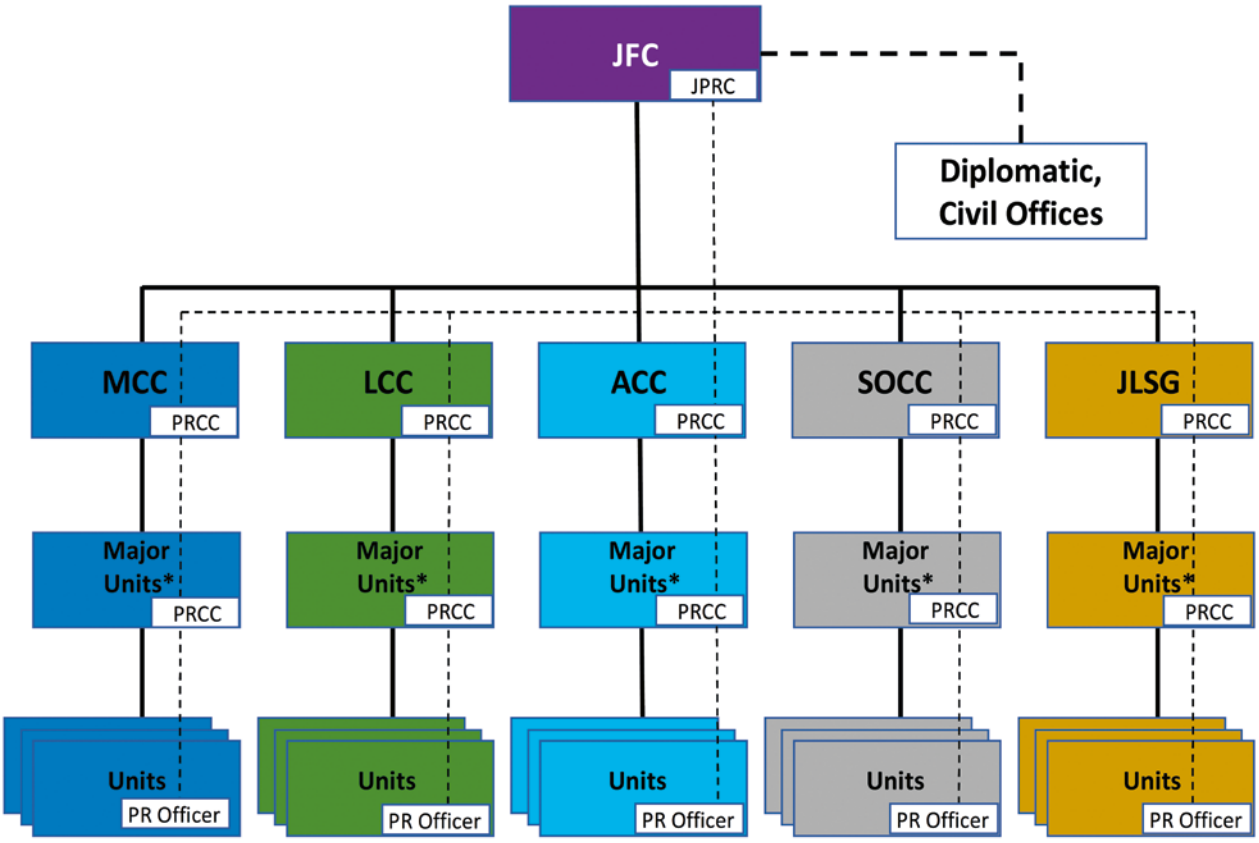
From a realist, operational standpoint, the need for combat reconstitution and sustainment strongly justifies JPR investment. Reconstitution includes recovering personnel and reintegrating them into operations where their experience remains vital. Experienced personnel, especially with recent combat experience, are not easily replaced via standard training. Their knowledge, awareness, and decision-making are critical, particularly during Major Combat Operations (MCO). An ISOP's value extends beyond morality to the Alliance's investment in its training and unique combat experience. Every captured, wounded, or missing NATO service member risks the loss of essential expertise, intelligence, and combat power.

For example, the F-35 program exemplifies multinational cohesion and advanced capability, as showcased by the training for its skilled pilots. Training an F-35 pilot costs approximately € 10 million and three years to achieve basic readiness – roughly the price of three main battle tanks – highlighting the value of such personnel.[8, 9, 10] The same applies to experienced NCOs, SOF, intelligence specialists, and other key enablers whose expertise is hard to develop.

Improve Alliance Synergy

NATO's 75th anniversary in 2024 demonstrated a unified alliance can sustain long-term peace and collective defence. Yet, the nature of warfare continues to evolve. Modern conflict is increasingly coalition-based, requiring unprecedented interoperability and ongoing combined training among allies. NATO leaders must see national forces as components of a collective structure, akin to the Allied Reaction Force (ARF), established in July 2024 to enhance deterrence.[11] Improved readiness, standardized training, and greater cohesion build trust, reduce the impact of personnel losses during MCO, and strengthen collective political security.

A coherent and robust JPR framework strengthens multinational trust and cohesion by enforcing standardized training, ensuring equipment compatibility, and enabling essential intelligence-sharing. An effective JPR system depends on routinely exercised, enforced standards. NATO JPR guidance, found in Allied Joint Publication (AJP) 3.7, *Recovery of Personnel in a Hostile Environment,* often lacks the tactical-level detail needed for effective execution.[12] For instance, no unified standard exists for survival gear, emergency radios, or signalling devices across NATO forces. These gaps create friction and delay recoveries – potentially costing lives. Incompatible communication systems hinder critical exchanges between ISOP, multinational recovery teams, and the JPRC, leading to breakdowns in mission information flow. NATO leaders must champion standardized JPR processes,



*Major Units: e.g. Corps, Division, Brigade, etc. and other services equivalents.

While the JPR organizational architecture is conceptually optimized for high-end warfighting, its peacetime implementation remains largely aspirational. The reliance on intermittent training and exercises, rather than persistent integration into baseline activities and current operations, has limited its practical utility and adaptability.

equipment, and training at the unit level – before Article 5 is triggered – to reinforce Alliance trust and readiness for major combat operations.

Establishing an Integrated JPRC

Allied Command Operations (ACO) leads Alliance missions, with SHAPE guiding three JFCs (Brunssum, Naples, Norfolk) and tactical commands (AIRCOM, LANDCOM, MARCOM). Throughout all these organizations, NATO lacks a single, dedicated institution responsible for the full JPR mission during peacetime. Instead, each of these five commands handles its own JPR activities. In crises, JPR responsibility typically shifts to a designated JFC and its ad hoc JPRC, which is often staffed informally by untraining personnel.[13]

No single NATO organization formally owns or champions JPR; responsibility remains dispersed under SHAPE's guidance. AIRCOM often serves as a key stakeholder and de facto SME hub, since many JPR functions like CSAR align with air operations and fall under the Military Committee Standardization Board.[14,15] Yet, the current Allied Joint Publication (AJP) 3.7 primarily covers CSAR – a vital, but incomplete, aspect of JPR. This leaves NATO without comprehensive joint doctrine for all JPR facets, such as non-conventional recovery or operations in denied areas where CSAR is impractical. Such a doctrinal gap has aggravated knowledge loss and hindered the shift from COIN to peer-conflict JPR.

To fix systemic issues, NATO should create a persistent, integrated JPRC as the central hub for doctrine, planning, and advocacy at SHAPE for strategic alignment. This JPRC needs a dedicated multinational SME staff covering all JPR disciplines (C2, intelligence, SERE, etc). JFC Brunssum – responsible for much of Central and Northern Europe and collective defence planning – is well suited to host it. In peacetime, it would develop doctrine, share lessons,

© US Marine Corps, Staff Sgt. Dengrier Baez

Romanian Marines from the 307th Naval Infantry Battalion conduct a beach landing during a JPR scenario in exercise Baltic Operations (BALTOPS) 2018.

source and prepare gear, and lead education and training. In crises, it would coordinate complex cross-area operations with expertise that ad hoc teams lack. Without this, the five commands lack a standardized, refined C2 function for full-spectrum JPR.

Investment in JPR Readiness

NATO's fragmented JPR efforts have sometimes weakened interoperability and readiness in multinational operations. No unified training syllabus or education program covers all NATO JPR forces across components, even for conventional CSAR. Groups like the Tactical Leadership Program (TLP), European Personnel Recovery Centre (EPRC), and European Air Group (EAG) play key roles in training, especially in the air domain, but are not formally within the NATO Command Structure. This can cause gaps in standardization and strategic alignment with SHAPE.[16] These organizations typically use AJP-3.7 as a foundation for CSAR training but generally don't cover the full JPR spectrum, including unconventional recovery or inter-agency coordination.

To provide a coherent JPR strategy and enhance readiness, the first step is establishing the aforementioned integrated JPRC as a focal point for JPR doctrine and advocacy. Subsequent efforts for a ready NATO JPR force must focus on education, training, and exercises:

Education: Many personnel retain a COIN-era JPR mindset (e.g., assuming air supremacy, neutral civilians). Forces need updated JPR education for peer A2/AD environments. This training must also cover the information warfare aspect, where adversaries may exploit ISOP for propaganda.

Training: While NATO air forces develop JPR skills through programs like TLP and the Air-Centric Personnel Recovery Operatives Course (APROC) at the EPRC, these focus mainly on traditional CSAR. Future training must cover multinational complexities, first responder integration, and non-traditional recovery methods.[17] Scenarios should include denied environments, advanced electronic warfare, and degraded C2.

Exercises: SHAPE-led exercises like STEADFAST DUEL, BALTOPS, and other major drills are necessary to test JPR functions at operational and strategic levels.[18] Exercises need challenging, JPR-focused objectives stressing the system; simple CSAR scripts are insufficient. NATO must prioritize JPR C2 resilience, interoperability, and decision-making under pressure before acquiring new assets. Without an integrated, trained JPR structure, even top CSAR platforms cannot overcome fractured C2. Exercises should also test deconfliction with other operations, managing multiple ISOP, and integrating non-military recovery options.

Conclusion

NATO leaders must re-energize JPR as a foundational NATO mission to ensure an isolated individual's worst day is not their last. Failing to adapt JPR would imperil future isolated personnel, like Lieutenant Colonel

Goldfein, and erode the Alliance's core strengths. A revitalized JPR capability is paramount because it upholds our unwavering moral contract with service members, fortifying their morale and resolve; it is crucial for reconstituting invaluable combat power and sustaining operational effectiveness; and it powerfully reinforces Alliance cohesion, deepening trust and bolstering collective security.

To achieve this, NATO must act decisively: establish an integrated, persistent JPRC with clear advocacy at SHAPE, and renew focus on comprehensive JPR doctrine, education, realistic multinational training, and demanding, large-scale exercises. Only through these efforts can NATO ensure 'that others may live,' safeguarding its greatest asset – its people – and maintaining its credibility as a defensive Alliance.[19] The time for incremental adjustments is over; a strategic reset for NATO JPR is essential. ●

1. Losey, Stephen. "'Start Finding Me, Boys" – Inside the Rescue of Lt. Col. Dave Goldfein.' *Air Force Times,* 19 June 2019, https://www.airforcetimes.com/news/your-air-force/2019/06/19/start-finding-me-boys-inside-the-rescue-of-lt-col-dave-goldfein/, (accessed 6 May 2025).
2. North Atlantic Treaty Organization. *NATO 2022 Strategic* Concept. NATO, 29 June 2022, https://www.nato.int/strategic-concept/, (accessed 8 February 2025).
3. Multination Capability Development Campaign. *Joint Personnel Recovery 2040: A Global Perspective.* Joint Personnel Recovery Agency, U.S. Joint Staff J7, 8 March 2021, pp. iv–vi.
4. Ibid, pp. 4–26.
5. Ibid, pp. 6–34.
6. Bausman, Charles. *Leave No Man Behind: Implications, Criticisms, and Rationale.* Mountain Tactical Institute, 2014, https://mtntactical.com/knowledge/leave-no-man-behind-implications-criticisms-rationale/, (accessed 8 February 2025).
7. North Atlantic Treaty Organization. AJP-3.7: Allied Joint Doctrine for Recovery of Personnel in a Hostile Environment. NATO Standardization Office, Edition B Version 1, March 2016.
8. McCarthy, Niall. 'The Cost of Training U.S. Air Force Fighter Pilots [Infographic].' *Forbes,* 9 April 2019, https://www.forbes.com/sites/niallmccarthy/2019/04/09/the-cost-of-training-u-s-air-force-fighter-pilots-infographic/, (accessed 9 November 2024).
9. Sanches, Miguel. 'Leopard 2: This is what the German battle tank costs.' Berliner Morgenpost, 13 May 2025, https://www.pogo.org/reports/armys-m1-tank-has-it-lived-up-to-expectations, (accessed 23 May 2025).
10. Lockheed Martin. *F-35 Fast Facts.* May 2023, https://www.lockheedmartin.com/content/dam/lockheed-martin/aero/f35/documents/May%202023%20F-35%20Fast%20Facts.pdf, (accessed 9 November 2025).
11. Supreme Headquarters Allied Powers Europe. 'Stand up of Allied Reaction Force Marks a New Era for NATO.' SHAPE News, July 2024, https://shape.nato.int/news-archive/2024/stand-up-of-allied-reaction-force-marks-a-new-era-for-nato, (accessed 19 April 2025).
12. North Atlantic Treaty Organization. AJP-3.7: Allied Joint Doctrine for Recovery of Personnel in a Hostile Environment. NATO Standardization Office, Edition B Version 1, March 2016.
13. Vuijk, Tim. *Interoperability: the key to leave no man behind.* Bachelor's thesis, Netherlands Defence Academy, 11 April 2019, pp. 26.
14. Magi, Andrea, and Javier Aguilar Gonzalez. *Joint Personnel Recovery in an Urban Environment.* Joint Air Power Competence Centre, August 2024, https://www.japcc.org/white-papers/joint-personnel-recovery-in-an-urban-environment/, (accessed 9 November 2025).
15. North Atlantic Treaty Organization (NATO) (2005), STANAG 3745 AMD (EDITION 4) – Medical Training and Equipment Requirements for Search and Rescue (SAR) and Combat Search and Rescue (CSAR) Missions, 17 May 2005.
16. Vuijk, Tim. *Interoperability: the key to leave no man behind.* Bachelor's thesis, Netherlands Defence Academy, 11 April 2019, pp. 27.
17. Winberg, Michael. 'Personnel Recovery and Unmanned Systems – Some Examples from Ukraine.' Kungl Krigsvetenskapsakademien, 28 January 2024, https://kkrva.se/personnel-recovery-and-unmanned-systems-some-examples-from-ukraine/, (accessed 6 May 2025).
18. Joint Warfare Centre, 'STEADFAST DUEL 2024: This Year's Largest NATO Command Post Exercise Concludes', 1 November 2024, https://www.jwc.nato.int/article/steadfast-duel-2024-concludes/, (accessed 24 May 2025).
19. O'Rourke, Patrick. 'Survival in Serbia.' Air & Space Forces Magazine, 9 March 2020, https://www.airandspaceforces.com/article/survival-in-serbia/, (accessed 19 April 2025).

ABOUT THE AUTHOR

Major Brennan Gallagher

US Air Force, HQ AIRCOM

Major Gallagher commissioned into the USAF in 2011 from the United States Air Force Academy and completed Specialized Undergraduate Pilot Training in 2012. He holds Weapons Officer and Evaluator qualifications in the HC-130J Combat King II. He has deployed multiple times to the Middle East and the Horn of Africa with personnel recovery task forces. A graduate of the National Intelligence University, he holds a bachelor's in Biology, a master's in Management, and a master's in Strategic Intelligence. Major Gallagher is a Senior Pilot with over 2,400 flight hours, including 240 combat hours, and currently serves as A35 Senior Planner Headquarters Allied Air Command.

Integrating the Blue and Green Domains

Evolving NATO Air-Land Integration for Multi-Domain Operations

By Lieutenant Colonel Erhan Güleç, TÜR Air Force, JAPCC
By Major Shawn Kelley, US Army, HQ AIRCOM

Military operations over the past century have witnessed a profound transformation, evolving from clashes dominated by single components to intricately synchronized joint and multi-domain endeavours. Within this evolution, the effective integration of air and land power – Air-Land Integration (ALI) – has become a cornerstone of operational success. Without true integration, air and land components risk desynchronization and suboptimal effectiveness, a danger highlighted by LTG Frederick Franks, Commander of United States VII Corps during Operation Desert Storm: 'I was free to nominate targets, but the correlation between those that we nominated and those that were struck was quite poor.'[1] To avoid repeating such shortfalls in a far more lethal future war, it is a strategic imperative that NATO creates and maintains a leading edge in ALI.

F-18s from the USS Gerald R. Ford aircraft carrier participate in a large-scale exercise, executing CAS missions with Turkish and US Joint Terminal Attack Controllers (JTACs) at a NATO-accredited JTAC school in Konya, Türkiye.

Historically, NATO developed a robust doctrine for air power contribution to counter-land operations (APCLO) in the 'former' Air-Land Battle concept. This doctrine encompassed a range of missions designed to leverage air power's speed, reach, and precision in support of land forces and degrade an adversary's ability to bring their land forces to bear. However, the operational landscape of the past two decades was dominated by Counterinsurgency (COIN) campaigns fought under conditions of assured friendly air superiority. For a generation of warfighters, these permissive conditions effectively reduced the broad concept of APCLO to its most frequent application: Close Air Support (CAS). While vital, this focus on CAS – engaging enemy forces near friendly troops – caused other APCLO concepts in the deeper tactical fight to atrophy.

Now, the threat of peer or near-peer adversaries equipped with advanced anti-access/area denial (A2/AD) systems capable of credibly contesting the air domain demands a fundamental shift in thinking. Future success hinges on the harmonious integration across the breadth of APCLO missions, complemented by a newly proposed land mission-set: Land Power Contribution to Counter-A2/AD (LPCA).

This article examines how NATO can ensure land commanders can leverage the full potential of air power, while air forces can harness land component capabilities – particularly long-range precision fires – to enable air operations in the modern battlefield. NATO's initial efforts to develop ALI is centred on three emerging concepts: the Joint Air Ground Integration Centre (JAGIC), the Air Support Operations Centre (ASOC), and the ASOC Battlespace Management Area (ABMA). Together, they provide the structural foundation to advance ALI and expand NATO's competency in Multi-Domain Operations (MDO).

Evolving Operational Realities: From Permissive CAS to Contested ALI

During the COIN era, land forces benefited immensely from reliable CAS, and the air forces grew accustomed

to delivering CAS in a low-risk environment. CAS was performed at generally low altitudes, where NATO militaries leveraged the psychological impact of visible air presence and its associated effects on morale for both friendly and enemy forces.

This period fostered significant advancements in CAS capabilities. NATO initiated the certification and qualification of Joint Terminal Attack Controllers (JTACs) through the NATO standardization process, ensuring a high degree of interoperability and competence in coordinating air strikes. Technological strides, such as the Digitally Aided Close Air Support (DACAS) system, improved the accuracy and responsiveness of CAS missions, while the proliferation of Unmanned Aircraft Systems (UAS) provided persistent surveillance and dynamic targeting capabilities. These developments matured NATO's CAS capabilities, proving highly effective within the specific context of permissive COIN environments.

However, these successes become liabilities if applied to future Large Scale Combat Operations (LSCO) against sophisticated adversaries, where the assumption of air supremacy evaporates. Peer adversaries will actively contest the air domain with integrated air defence systems (IADS), electronic warfare (EW), and fighter aircraft, increasing the risk to NATO aircraft. Furthermore, the scale of LSCO will likely generate simultaneous troops-in-contact (TIC) events across vast areas, creating a demand for air power that may exceed availability in a contested environment.

Navigating this new reality requires a paradigm shift in risk acceptance and a move beyond treating ALI as a euphemism for 'air support.' Instead, ALI is about systematically integrating APCLO and LPCA principles based on the appreciation of the mutual benefit each domain can offer the other. For example, relying solely on air power to suppress A2/AD threats while also providing APCLO is likely untenable, especially in the

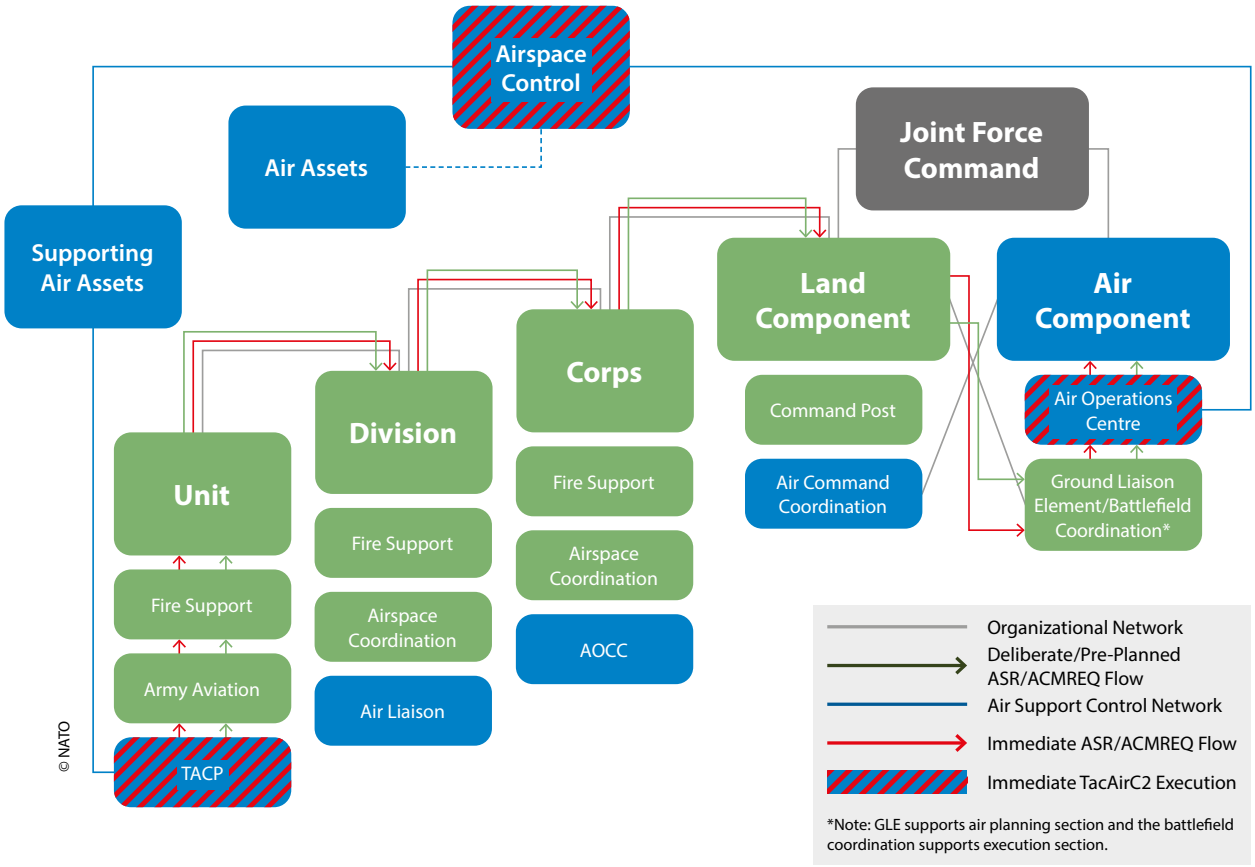


Figure 1: *NATO's Current Airspace Control Structure and Airspace Request Network.[2] A 2022 analysis suggests an integration gap exists at the corps level.*

opening phases of a conflict. Instead, land-based long-range precision fires, such as the existing Army Tactical Missile System (ATACMS) and the forthcoming Precision Strike Missile (PRSM), alongside other land effects (e.g. EW, intelligence, surveillance, reconnaissance (ISR), and cyber), must be integrated into the counter-A2/AD fight. LPCA must proactively shape the environment to enable air operations, reducing the burden on air assets and creating windows of opportunity for APCLO missions where they are most needed.

Bridging the Gaps: Recent NATO Efforts to Revitalize ALI

Recognizing the urgency, Allied Land Command (LANDCOM) and Allied Air Command (AIRCOM) have intensified efforts to revitalize ALI. A key catalyst was the 2020 Joint Analysis and Lessons Learned Centre (JALLC) report on ALI, which concluded that NATO's existing Tactical Air Command and Control (TacAirC2) architecture was potentially unsuitable for LSCO and recommended extending its execution capabilities to the warfighting corps (WFC).

Acting on these findings, NATO established the Battlefield Coordination Detachment (BCD) at AIRCOM in 2022 to enhance daily liaison. In 2024, the NATO ALI Forum was created to synchronize efforts in support of the MDO concept, resulting in the 'Making NATO ALI Ready 2024–2026' plan. This roadmap outlines five key lines of effort (LOEs): command and control (C2), Counter-A2/AD (linking APCLO and LPCA), APCLO, airspace management (ASM), and integrated air and missile defence (IAMD). The formal ratification of the ALI Forum Charter by the Deputy Commanders of both AIRCOM and LANDCOM underscored the high-level commitment to this key effort.

Developing Core Concepts for ALI: JAGIC, ASOC, and ABMA

The JAGIC, ASOC, and ABMA concepts are central to developing NATO's future ALI framework. Though still under refinement, they represent a significant evolution in synchronizing air and land power.

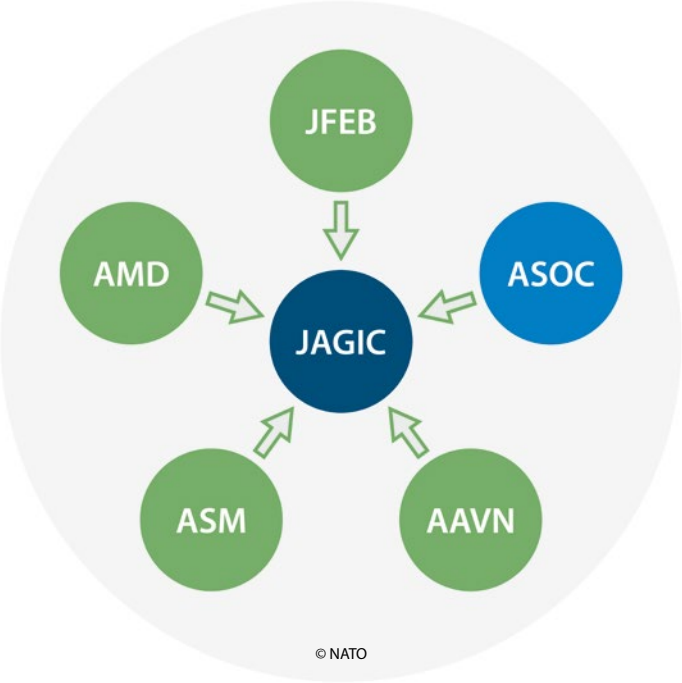


***Figure 2:** Typical JAGIC Execution Cell Composition, as discussed below.[3]*

'The integration of NATO's air and land capabilities – the "blue" and "green" domains – is a strategic necessity for maintaining credible deterrence in an era of renewed great power competition.'

1. JAGIC Concept

The JAGIC was developed based on lessons learned from Operation Anaconda and other missions in Afghanistan and Iraq. The JAGIC is a method of organizing personnel and equipment at the highest tactical echelon, in NATO typically the WFC, to foster teamwork between components. Its core membership includes representatives from the ASOC (air execution), surface fires, ASM, air and missile defence (AMD), and Army aviation (AAVN). This co-location and integration enable the rapid coordination, synchronization, and execution of joint fires. The JAGIC's effectiveness hinges on this fusion, providing the Corps commander with a scalable, joint team enabling rapid decision making while minimizing fratricide risk. Since 2021, LANDCOM and AIRCOM have collaborated on developing and testing the JAGIC concept within NATO exercises, refining its structure and procedures, and advancing the concept with each exercise.

2. ASOC Concept

The ASOC is the Air Component's team of experts embedded in the JAGIC, tasked with controlling air operations within an assigned airspace. It serves as the primary decentralized execution element for air power supporting the WFC, embodying the tenet that tactical decisions are best made by those closest to the fight. Unlike an Air Operations Coordination Centre (AOCC), which plans future operations, the ASOC's primary mission is the real-time execution of air missions, managing immediate air requests, and providing fused air/ground situational awareness.

The ASOC's key tasks include: exercising tactical control of assigned aircraft operating within the ABMA, coordinating with adjacent TacAirC2 agencies and airspace users, managing the Joint Air Request Net (JARN) for immediate CAS requests, providing fused air/ground situational awareness via voice communications and tactical data links (TDLs), integrating joint suppression of enemy air defences (J-SEAD) effects, and processing immediate air support requests (ASRs). Within NATO, the Deployable Air Command and Control Centre (DACCC) holds the responsibility for developing and implementing the NATO ASOC capability.

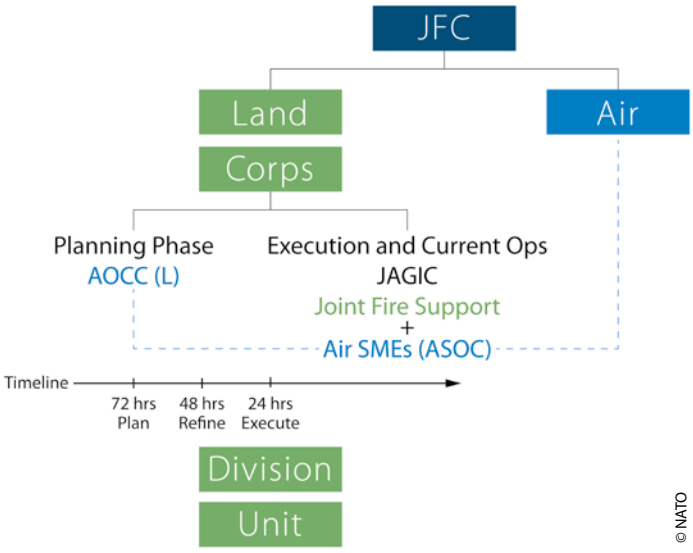


***Figure 3:** ASOC Command Relationships.*[4]

3. ABMA Concept

The ABMA is a proposed volume of airspace assigned to the WFC, with control authority delegated from the Airspace Control Authority (ACA) to the ASOC. Within an ABMA, the ASOC manages assigned air assets and deconflicts all airspace users, including friendly aircraft, UAS, and ordnance (artillery, missiles), enabling the WFC commander to rapidly execute organic fires and aviation operations *without* requiring further coordination with the ACA for each specific mission.

The ABMA dimensions are flexible. However, they will generally be defined laterally by the boundaries of the WFC, longitudinally from the WFC rear area to the fires support coordination line (FSCL), and vertically from the ground up to the maximum ordinate (MAXORD) of the preponderance of cannon artillery. The ABMA's ceiling is referred to as the coordinating altitude (CA) to maintain maximum interoperability. The ABMA's dimensions are defined and implemented in the Air Component's Air Tasking Order/Airspace Control Order (ATO/ACO). The ABMA is flexible, and its dimensions can be dynamically adjusted in real time via coordination with the ACA based on the tactical situation, ASOC capabilities, and overall air picture.

By delegating control to the ASOC, the ABMA differs from a high density airspace control zone (HIDACZ), where control is retained by the ACA, and promises to drastically reduce the time needed to clear airspace for dynamic joint fires.

Integration in Action

These three concepts are designed to work in concert. The JAGIC provides the integrated C2 hub within the Corps HQ. The ASOC, nested within the JAGIC, provides the specialized air C2 execution capability. The ABMA provides the defined airspace within which the ASOC can exercise its delegated authority. This setup promises to achieve rapid synchronization and deconfliction of air and surface effects reducing the time needed to clear airspace for dynamic joint fires.

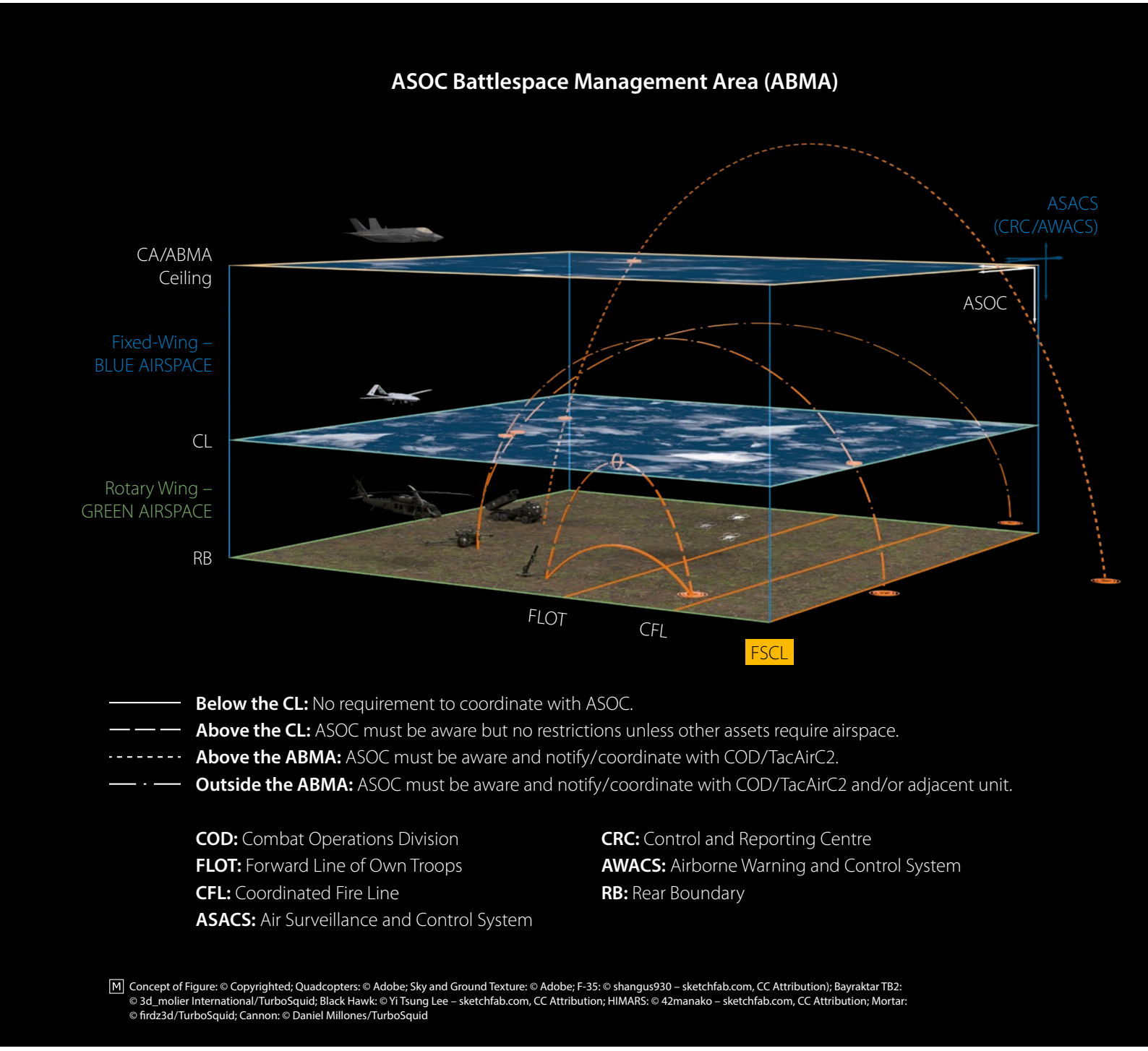


Figure 4: *Depiction of the ABMA Concept: a volume of airspace typically aligned with the Warfighting Corps' lateral and vertical boundaries (CL to CA). Control authority within the ABMA is delegated from the Airspace Control Authority (ACA) to the ASOC located within the Corps' JAGIC.*

ALI: Preparing an MDO-Capable Force in the Context of A2/AD

Effective ALI, realized through concepts like JAGIC, ASOC, and ABMA, is a critical enabler for NATO's broader ambition of achieving an MDO-capable force structure. MDO requires the seamless integration of capabilities beyond air and land, including maritime, space, cyber to create converging effects that overwhelm an adversary.

In the context of Counter-A2/AD, this ALI paradigm shift is vital. By integrating LPCA through the JAGIC, land forces can degrade enemy IADS, creating localized windows of air superiority or parity that allow APCLO missions to be conducted with acceptable risk. This demands a sophisticated understanding of cross-domain cueing: for example, land-based EW detecting a radar, space capabilities providing an accurate location, followed by a prompt artillery strike coordinated through the JAGIC, enabling follow-on air strikes or reconnaissance managed by the ASOC.

This integrated approach necessitates a dynamic balancing act throughout a campaign. The opening stages might heavily emphasize LPCA to degrade A2/AD systems and establish conditions for air power, potentially meaning fewer APCLO sorties directly supporting ground manoeuvre. Staffs must accept this potentially asymmetric initial contribution, understanding that land assets targeting key A2/AD nodes directly enable future air support. As the A2/AD threat is suppressed and a more favourable air situation is achieved, the balance will shift, enabling a greater weight of effort towards APCLO missions to support the land scheme of manoeuvre.

Recommendations for the Way Forward

Achieving comprehensive ALI requires sustained institutional change. While progress is being made, significant work remains. The following recommendations are crucial for advancing this topic within NATO:

Define and Codify: Formally agree on a NATO definition for ALI that reflects its modern, integrated, multi-domain context. The following is offered as a starting point for discussion: *ALI is the application of Air and Land Component capabilities, coordinated and synchronized across domains, to achieve complementary and reinforcing effects that enable Joint Force objectives.* This definition could stimulate conversation to support further development and direction of ALI and increase our lethality in the tactical deep fight. As Lieutenant General Sean Bernabe, Deputy Commander of United States Army Europe and Africa, has noted, 'If we only used organic [land] options, it limits our ability to fight. Mass can be delivered by apportioned joint effects.'[5]

Update Supporting Doctrine and TTPs: Update AJP-3.3.2 *Close Air Support and Air Interdiction* to broaden its scope and fully incorporate the spectrum of APCLO missions within the new ALI framework. Amend AJP-3.3.5 *Airspace Control* to include the ABMA concept, associated procedures, and delegation parameters. Update relevant ATPs (e.g., ATP-3.3.2.1, ATP-3.3.5.1) to provide the detailed 'how-to' guidance aligned with the updated AJPs.

Continue Experimentation and Refinement: Leverage NATO exercises, wargames, and experimentation venues to rigorously test and refine the JAGIC, ASOC, and ABMA concepts. Establish robust feedback mechanisms to capture lessons learned and rapidly iterate on doctrine, TTPs, and organizational structures. Ensure Component Commands and subordinate Corps HQs actively participate and develop proficiency.

Ensure Interoperability: Conduct comprehensive capability studies to identify requirements and ensure the necessary C2 systems, communication networks, TDLs, and situational awareness tools used within the JAGIC and by the ASOC are interoperable with existing and future NATO standards. Prioritize solutions that enable seamless digital information exchange between air and land platforms and command nodes.

Institutionalize Training and Certification: Once JAGIC, ASOC, and ABMA are formally institutionalized in NATO doctrine, develop standard training and certification requirements to ensure the force is ready to execute.

Foster a Joint Culture: Promote education, cross-component assignments, and integrated training opportunities to break down cultural barriers and foster the mutual trust and understanding for effective ALI.

Conclusion

The integration of NATO's air and land capabilities – the 'blue' and 'green' domains – is a strategic necessity for maintaining credible deterrence in an era of renewed great power competition. Victory against peer adversaries requires a shift away from component-centric

'Military operations over the past century have witnessed a profound transformation, evolving from clashes dominated by single components to intricately synchronized joint and multi-domain endeavours.'

operations and legacy models optimized for permissive environments. NATO must embrace a comprehensive, effects-based approach to ALI, moving beyond the recent focus on CAS.

The development and refinement of the JAGIC, ASOC, and ABMA concepts offer a pathway to synchronize APCLO and LPCA, enabling commanders to generate integrated joint effects at the speed and scale required by LSCO within an MDO framework. While recent initiatives by AIRCOM, LANDCOM, and the wider NATO community have generated positive momentum, significant work remains. Fully realizing the potential of modern ALI requires sustained commitment from strategic leaders and a truly integrated joint mindset down to the tactical level. ●

1. McCaffrey, J, T., *Air University,* [website], 2004, https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/CP_0017_MCCAFFREY_BATTLEFIELD_AIR_INTERDICTION.PDF, (accessed 14 April 2024).
2. NATO JALLC, [website], 2020, https://www.jallc.nato.int/application/files/9916/0503/5926/Factsheet_ALI.pdf, (accessed 9 May 2025).
3. NATO ASOC Operating Handbook, 2024.
4. Ibid.
5. MCLCC Commanders Conference, HQ, LANDCOM, 29 October 2024.

ABOUT THE AUTHORS

Lieutenant Colonel Erhan Güleç
TÜR Air Force, JAPCC

Lieutenant Colonel Erhan Güleç graduated from the Turkish Air Force Academy in 2005 with a bachelor's degree in electronic engineering and was stationed as an Intercept Controller (IC) at the Control and Reporting Centre (CRC) of Diyarbakir, Türkiye. Following his master's degree in electronic engineering, in 2013, he joined the Airborne Early Warning and Control (AEW&C) Peace Eagle initiative in Seattle, USA. Upon his completion of the training programme, he worked as a Weapon Controller and Fighter Allocator in E7-T AEW&C Konya, Türkiye.

In 2018, he joined the CRC of Çanakkale, Türkiye and served as a Mission Commander (MC).

Since August 2023, he has been serving as a Close Air Support/Joint Terminal Attack Controller (CAS/JTAC) Subject Matter Expert in the Combat Air Branch of the JAPCC.

Major Shawn Kelley
US Army, AIRCOM

Major Kelley is the Executive Officer of the NATO Battlefield Coordination Detachment, at Allied Air Command, Ramstein, Germany. He is an Artilleryman and SME in Air and Land Integration, and the primary development officer of the ALI Forum, NATO's foremost effort in integrating the Air and Land domains. Before this role, MAJ Kelley was an Advisor to the Nation of Georgia's Defence Forces, helping develop modern training and doctrine programmes. Other previous assignments include Armistice compliance inspection in the Demilitarized Zone between North Korea and South Korea; Chief Targeting Officer at LANDCOM, Izmir, Türkiye; and principal staff trainer in the Artillery Battalion of the King Abdulaziz Mechanized Brigade, Al Hofuf, Saudi Arabia. Major Kelley has multiple combat deployments to Iraq and Afghanistan; he has also worked in several programmes of the Ukraine Security Assistance Initiative.

A Russian Su-34 takes off with electronic countermeasures on the wingtips.

Beyond the Hype

Assessing Russian Airborne EW Shortcomings in the Ukraine Conflict

By Lieutenant Colonel Athanasios Sdrakas, GRC Air Force, JAPCC

Author's note: This is a non-classified article, and as such, some technical details and conclusions are omitted. NATO members are encouraged to reference JAPCC's secure website for a more complete analysis.

Throughout the Russo-Ukrainian conflict, the Russian Aerospace Forces (VKS) have suffered significant combat aircraft losses, illuminating vulnerabilities in their airborne Electronic Warfare (EW) capabilities. Despite their long-held reputation for proficiency in the electromagnetic spectrum (EMS), the VKS has sustained extensive aircraft attrition. This includes high-value assets (HVAs) such as two Beriev A-50U 'Mainstay' airborne early warning and control (AEW&C) platforms, lost within a month in early 2024, and numerous Sukhoi Su-34 'Fullback' strike fighters–reportedly nearly a quarter of the pre-war fleet. The destruction of the A-50s, with their low numbers and highly specialised crews, dealt a severe blow to Russia's operational reach and situational awareness.[1] While the precise financial impact is difficult to assess, the sheer number of aircraft lost is comparable to a decade of peacetime military aircraft production, underscoring the severity of these setbacks.[2]

These losses, inflicted by a combination of legacy Soviet-era air defence systems like the S-200 (SA-5 'Gammon') and Buk-M1 (SA-11 'Gadfly'), alongside modern Western-supplied systems such as Patriot, National Advanced Surface-to-Air Missile Systems (NASAMS), and IRIS-T SLM, indicate systemic failures in Russian airborne EW.[3] The VKS has demonstrably struggled to deploy effective EW countermeasures to protect its assets, even against known threats. The Su-34, one of Russia's most advanced tactical aircraft equipped with sophisticated EW suites like the Khibiny, exemplifies this failure, with over thirty-five reportedly downed by Ukrainian air defences.[4] This inability to effectively shield aircraft raises profound questions about the development, integration, and operational employment of Russian airborne EW. This paper will assess the doctrinal underpinnings of Russia's reliance on EW, analyse the systemic and operational shortfalls observed in Ukraine, and consider the implications for Russian military adaptation and NATO's strategic posture.

Russia's Doctrinal Bet on EW: An Asymmetric Counter to Low Observable (LO) Technology

Russia's emphasis on EW, or Radio-Electronic Combat (REB) in its doctrine, is not accidental but a deliberate strategic choice rooted in the post-Cold War technological landscape. Faced with the West's, particularly the United States', growing dominance in LO technology – exemplified by aircraft like the F-117A Nighthawk, B-2 Spirit, and later, the F-22 Raptor and F-35 Lightning II, Russia recognised its limitations in developing comparable LO platforms. A combination of an underdeveloped civilian electronics sector, lack of advanced precision manufacturing tools, industrial limitations, lagging composite material science, and persistent financial constraints hampered its LO technology ambitions, leading to the abandonment of early projects like the Mikoyan MiG 1.44 and Sukhoi Su-47 Berkut.[5]

System Name	NATO Reporting Name	Origin	Notable Capabilities	Remarks
S-300PS /PMU	SA-10 'Grumble'	Soviet Union	Long-range SAM (75–200 km), high-altitude engagement	Several Russian aircraft reportedly downed by these legacy systems, which are still in Ukrainian service
Buk-M1 /M1-2	SA-11 'Gadfly'	Soviet Union	Medium-range (30–50 km), mobile SAM	Used in multiple ambushes against low-flying Russian jets
S-125 Pechora	SA-3/SA-5 hybrid	Soviet Union / Ukraine upgrades	Digital upgrades: effective against slow or low-flying targets.	Ukraine adapted Pechora for more flexible battlefield use.
NASAMS	—	Norway/USA	Networked, radar-guided, medium-range SAM	Designed to intercept aircraft, helicopters, UAVs, and cruise missile.
IRIS-T SLM	—	Germany	Short-to-medium-range, high precision	Effective against cruise missiles and tactical aircraft
Patriot PAC-2/3	—	USA	Advanced radar, hit-to-kill capability	Used to target high-value aircraft like the A-50 AEW&C

Table: Key Ukrainian Air Defence Systems Used Against Russian Aircraft.[25]

Russian military thought, influenced by concepts of a 'revolution in military affairs' and the perceived efficacy of countermeasures, posited that LO technology was a solvable technical challenge.[6] Consequently, Russia pursued an asymmetric strategy, prioritizing robust EW capabilities to degrade adversary sensor networks and protect its own, less LO, assets. This doctrine viewed EW as a protective adjunct and a central pillar of combat operations, designed to disrupt enemy Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems.[7] The downing of an F-117A over Serbia in 1999 by a Serbian SA-3 Goa, reportedly aided by older Soviet radar techniques and intelligence, further solidified Russian confidence in their ability to counter LO technology through sophisticated air defence and EW.[8]

Key industrial defence players like the Concern Radio-Electronic Technologies (KRET) and design bureaus such as the Central Scientific-Research Institute for Radio Engineering (TsNIRTI) and the Kaluga Scientific-Research Institute for Radio Engineering (KNIRTI) spearheaded the development of advanced airborne EW systems. Notable examples include the KNIRTI L005S Sorbsiya pods for Su-27/30 aircraft and the more recent L-175 Khibiny family of systems, designed for platforms like the Su-30SM, Su-34, and Su-35. The Khibiny was touted as a sophisticated system, purportedly upgraded based on experiences in Syria, capable of jamming enemy radars and cueing anti-radiation missiles. This doctrinal reliance and industrial focus created an expectation of airborne EW dominance that has been severely tested in Ukraine.[9]

Operational Shortfalls and Systemic Failures in Russian Airborne EW

Despite possessing a diverse pre-war inventory of airborne EW assets, Russia's performance in Ukraine has fallen short, failing to meet doctrinal expectations by protecting VKS assets. At the outset, Russian EW achieved some initial success in degrading Ukrainian Ground-Based Air Defence (GBAD) units. However, this advantage proved short-lived, as Ukrainian air defences demonstrated resilience and adaptability. In a manner of weeks, they had repositioned assets, reset radar systems, and restored air defence coordination, diminishing the impact of Russian EW.[10] The three leading causes of failure include:

1. **Lack of Integrated SEAD/DEAD Operations:** One fundamental failure has been the inability to effectively integrate airborne EW assets into cohesive Suppression or Destruction of Enemy Air Defences (SEAD/DEAD) campaigns. Russian airborne EW platforms, such as the Il-20M 'Coot' surveillance aircraft and Su-34s equipped with anti-radiation missiles (ARMs) like the Kh-31P and Kh-58, frequently operated without dynamic coordination with GBAD suppression efforts, artillery, or other air units. This lack of integration allowed Ukrainian SAMs, employing agile 'pop-up' tactics with independently operating Buk Transporter Erector Launchers and Radar (TELARs), to complicate Russian targeting and undermine the effectiveness of reactive ARM employment and EW.[11]

2. **Fragmented Command and Control (C2) and Data Fusion:** Limited airborne C2 and data fusion capabilities have further hampered Russian EW effectiveness. Russian airborne EW and surveillance platforms like the Il-20M suffered from poor data dissemination. Communication methods introduced latency and reduced operational tempo, while Russia's fragmented C2 structure hindered real-time EW coordination and prevented dynamic retaking of EW effects.[12] Russia's heavily centralised C2 significantly limited the flexibility of its airborne EW assets. In contrast, Ukraine's more decentralised, NATO-influenced approach led to effective counter-jamming measures, frequent repositioning of assets, use of frequency-hopping spread spectrum (FHSS) techniques, and closer EW coordination with manoeuvre elements.[13]

3. **Technical and Integration Deficiencies:**

- System Limitations: The Khibiny system, a digital radio-frequency memory (DRFM)-based jammer, primarily relies on generating powerful noise or deception jamming signals to overpower enemy radars. While potentially effective against older radar systems, this

Wreckage of Russian Su-35S (RF-81771), downed despite advanced EW systems.

approach is less successful against modern agile radars employing sophisticated frequency-hopping techniques and advanced signal processing.[14]

- Platform Integration Issues: The physical characteristics of some EW pods, such as the SAP-14 'Stavropol' escort jamming pod intended for strike fighters, reportedly introduce considerable aerodynamic drag, reducing aircraft range and endurance, thereby limiting their operational utility on specific missions.[15]
- Avionics Conflicts: A persistent weakness, stemming from an ageing defence industrial structure that often separates radar and EW design teams, has been the poor integration of EW systems with other onboard avionics. On some Russian aircraft, pilots reportedly must choose between activating their radar for targeting or ground mapping and employing their EW self-protection suite, creating critical vulnerabilities, particularly for aircraft like the Su-34 operating in contested airspace. While there are reports of Khibiny system modernizations aimed at minimizing pilot workload, their widespread implementation and effectiveness remain unclear.[16]
- Electromagnetic Interference: Poor coordination and deconfliction of EW activities, exacerbated by deficiencies in communications and radio discipline among Russian forces, led to instances of electromagnetic interference. Reports of self-inflicted degradation indicate that Russian jammers, intended to disrupt Ukrainian systems, likely interfered with their own communications and C2 networks. This reportedly led to a reduction of some EW operations early in the invasion, allowing Ukrainian air defences to regain the initiative.[17]

These operational and technical shortfalls reveal deeper systemic problems: rigid command structures unsuited to dynamic electromagnetic environments, persistent defence industry issues impacting quality and innovation in airborne systems, and inadequate training for complex, contested electromagnetic operations.

For example, the VKS's traditionally hierarchical and centralised C2 system hindered the agility required for modern EMS operations. In a domain in which success or failure is determined at machine speed, a system reliant

Russian SAP-14 escort jamming pod on display – designed for Su-34/35 to disrupt enemy radar.

on rigid chains of command for approval or coordination inherently introduces delays and stifles local initiative. This contrasts with the more distributed C2 models increasingly favoured by Western air forces, which empower lower echelons with greater decision-making authority within defined parameters. Such rigidity not only slows reaction times to fleeting EW opportunities or threats but also makes it challenging to deconflict friendly EMS activities effectively, potentially exacerbating issues like electromagnetic fratricide and limiting the ability to orchestrate a cohesive, theatre-wide electromagnetic battle plan. The observed difficulties in integrating airborne EW with SEAD/DEAD efforts are a clear manifestation of this systemic C2 challenge.

Furthermore, long-standing issues within the Russian defence industrial base (MIC) contributed to the observed shortcomings. While capable of producing sophisticated individual platforms and systems in theory, the MIC has, according to multiple open-source analyses, struggled with consistent quality control, systems integration, and the incorporation of innovative technologies, particularly in microelectronics. This can lead to airborne EW systems that may perform well in controlled test environments but underperform or exhibit unexpected vulnerabilities under the stresses of real-world combat. The avionics integration challenges, which force pilots into difficult operational compromises, are indicative of these deeper industrial and design problems.

'NATO must not misinterpret these failures as indicative of a permanent or insurmountable systemic flaw. Russia's long military history demonstrates an ability to adapt, particularly when confronted with significant operational setbacks. Complacency within NATO would be a strategic error.'

Finally, inadequate training likely compounds these material and structural deficiencies. Effective operations in a densely contested EMS require highly specialised training for pilots, EW officers, and planners. This includes not only proficiency in operating specific equipment but also a deep understanding of adversary capabilities, joint EMS C2 procedures, and tactics for operating in degraded conditions. Reports

German IRIS-T SLM air defence system – capable of countering aircraft, missiles, and drones with networked radar and ECM resistance, posing a serious challenge to Russian EW assets.

of Russian units exhibiting poor communications discipline or struggling with encrypted systems suggest potential gaps in basic EMS operational preparedness. If training scenarios do not accurately replicate the complexity and dynamism of modern electromagnetic warfare, or if they fail to adequately stress combined arms coordination in the EMS, then even advanced equipment may be poorly utilised, leading to the underperformance observed in Ukraine. The failure to adapt EW tactics in response to Ukrainian countermeasures further suggests that VKS training may not foster the cognitive flexibility and problem-solving skills required by personnel in this domain.

Strategic Implications for NATO

The war in Ukraine has demonstrated that Russia's once lauded airborne EW capabilities, while possessing some strengths, have suffered from doctrinal, technical, and operational weaknesses. In the three-year conflict, Russian airborne systems have frequently underperformed, failing to protect high-value platforms or achieve localised electromagnetic superiority against a determined and adaptive adversary. Vulnerabilities in C2, inter-service integration, technical limitations against modern threats, and an overreliance on brute-force jamming techniques have contributed to significant VKS losses.

For NATO and its partners, these developments carry dual significance. First, the conflict has challenged pre-war notions of overwhelming Russian EW dominance in the airborne domain. Its weaknesses offer potentially exploitable seams should the Alliance ever face a direct confrontation.

Secondly, and more importantly, NATO must not misinterpret these failures as indicative of a permanent or insurmountable systemic flaw. Russia's long military history demonstrates an ability to adapt, particularly when confronted with significant operational setbacks. Its EW systems, doctrine, and training will undoubtedly evolve based on the harsh lessons from Ukraine. Complacency within NATO would be a strategic error. Instead, the Alliance must accelerate its efforts to achieve and maintain superiority across the electromagnetic spectrum. NATO must prioritize several areas:

A Russian Su-30SM fighter outfitted with wingtip-mounted Khibiny-U EW pods.

1. **Robust SEAD/DEAD and Counter-Anti-Access/Area Denial (A2/AD):** Russia's difficulties in executing effective SEAD do not diminish the growing threat posed by integrated A2/AD systems globally. NATO must continue to modernize its own SEAD/DEAD capabilities, doctrine, and training, fully integrating EW as a core component rather than an isolated supporting function.[18]

2. **Resilience, Agility, and Adaptability:** The Ukrainian experience underscores the value of Agile Combat Employment (ACE), resilient and distributed C2 architectures, and rapid institutional adaptation. NATO forces must be capable of operating effectively in degraded and disputed EMS environments.[19]

3. **Reinforce Doctrinal and Technical Interoperability Across the EMS:** Effective multi-domain operations require seamless EMS integration across air, land, sea, space, and cyber domains. NATO should accelerate the refinement of joint electromagnetic manoeuvre warfare concepts and invest in capabilities that enhance interoperability.[20]

4. **Capability Portfolio Rebalance:** The conflict challenges over-reliance on many 'exquisite,' high-cost platforms. A balance with sufficient mass of 'precise enough,' cost-effective systems, including munitions, drones, and EW platforms, is necessary for sustained high-intensity operations.[21]

5. **Training for EMS-Contested Environments:** NATO aircrews, accustomed to permissive environments, must train rigorously for high-intensity combat where the EMS is heavily contested, and losses are a realistic possibility. Training scenarios must reflect the degraded C2 and ISR conditions likely to be encountered against a peer adversary with functioning EW assets.[22]

6. **Invest in Advanced, Adaptive EW Capabilities:** The limitations of some Russian systems against agile, modern radars underscore NATO's need for advanced, adaptive, EW.[23] It must invest in distributed, networked, and resilient EW solutions, and continue advancing software-defined and AI-driven solutions that remain capable in a complex EMS.[24]

The Ukraine war should serve as an inflection point, not a final judgment on Russian EW capabilities. NATO's strategic posture must anticipate that Russia will adapt and redouble its goals of EMS superiority, and NATO must find its own lessons in Russia's shortcomings. This will involve a self-reflective look on its

own EW technology, institutional agility, doctrinal innovation, and operational flexibility. This ongoing challenge demands sustained investment and a unified approach across the Alliance to ensure that NATO retains its edge. The struggle for dominance in the electromagnetic spectrum will be a defining feature of future conflicts. ●

1. Suciu, P., 'Russia Can't Hide the Fact Its Air Force Is Taking Heavy Losses in Ukraine', The National Interest, 12 October 2024, (accessed 14 February 2025).
2. Bronk, J., 'Airborne Electromagnetic Warfare is Critical for NATO's Airpower Edge', Royal United Services Institute, 24 October 2024, (accessed 16 February 2025).
3. Ibid.
4. McCrory, D., 'Electronic Warfare in Ukraine: Preliminary Lessons for NATO Air Power Capability Development', JAPCC Journal 36, October 2023, (accessed 18 February 2025).
5. Kofman, Michael & Thomas, Jeffrey, 'Russian Military Strategy: Core Tenets and Operational Concepts.' Centre for Naval Analyses (CNA), August 2021, (accessed 19 May 2025).
6. Balestrieri, S., 'Russia's New PAK DA Stealth Bomber Nightmare Has Just Landed', 1945, 14 February 2025, (accessed 20 March 2025).
7. Mc Dermott, R., 'Electronic Warfare in Contemporary Russian Military Thought'. The Jamestown Foundation, 27 June 2022, (accessed 24 March 2025).
8. Plopsky, G., & McDermott, R., 'Moscow's Perspectives on the Evolution of US Stealth Technology', Wavell Room, 2 May 2019, (accessed 20 February 2025).
9. Bronk, J., Reynolds, N., & Watling, J. 'The Russian Air War and Ukrainian Requirements for Air Defence, RUSI Special Report', 7 November 2022, (accessed 20 May 2025).
10. Military & Defence, 'Russian forces were suffering from ‚electronic fratricide' within days of attacking Ukraine, a new report says', Business Insider, 21 November 2022, (accessed 10 April 2025).
11. Ibid 9.
12. Ibid 9.
13. Ibid 9.
14. Johnson, R., 'Russian EW Weaknesses Endure While Other Nations Innovate', AIN, 16 June 2019, (accessed 30 April 2025).
15. JSTOR, 'The Heavyweight Component', 1 Jan 2016, (accessed 30 April 2025).
16. Top War, 'The Ministry of Defense decided to modernise the Khibiny electronic warfare complex based on the results of using Su-34 front-line bombers in the NVO in Ukraine', 23 May 2022, (accessed 10 April 2025).
17. Ibid 9.
18. Ibid 9.
19. Withington, Thomas, 'Russian Electronic Warfare: From History to Modern Battlefield', IWI, 21 March 2024, (accessed 20 May 2025).
20. JAPCC, 'Electromagnetic Operations in NATO: The Evolving Role of EW and EMS Superiority', 2023, Joint Air Power Competence Centre, (accessed 21 May 2025).
21. Ibid 19.
22. McDermott, Roger, 'Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum', September 2017, International Centre for Defence and Security, EESTI Estonia, (accessed 21 May 2025).
23. ISW, 'Russian Offensive Campaign Assessment', 9 April 2025, (accessed 20 May 2025).
24. Bronk, Justin, 'Airborne Electromagnetic Warfare in NATO: A Critical European Capability Gap', RUSI, (Accessed 20 May 2025).
25. Di Mizio, G., Gjerstad, M. 'Ukraine's Ground-Based Air Defence: Evolution, Resilience and Pressure,' [website], International Institute for Strategic Studies, 2025, https://www.iiss.org/online-analysis/military-balance/2025/02/ukraines-ground-based-air-defence-evolution-resilience-and-pressure/#:~:text=Evolving%20inventory,to%20counter%20Russian%20missile%20attacks (accessed 18 Aug 2025).

ABOUT THE AUTHOR

Lieutenant Colonel Athanasios Sdrakas

GRC Air Force, JAPCC

Lieutenant Colonel Athanasios Sdrakas graduated from the Hellenic Air Force Academy with a Bachelor of Science in Aeronautics in 2000. He holds two Master of Science degrees: one in International Affairs from the University of Nicosia, Cyprus, and another in Environmental, Disaster, and Crisis Management Strategies from the National and Kapodistrian University of Athens. He began his service in the 348 Tactical Reconnaissance Squadron as a fighter pilot from 2000 to 2009, accumulating over 1,000 flying hours on the RF-4E aircraft. Subsequently, he was an instructor pilot in the 364 Air Training Squadron from 2009 to 2022, accumulating nearly 3,000 flying hours on the T-6A aircraft and serving as a squadron commander. He graduated from the Fighter Weapons School and the Supreme Joint War College. Lieutenant Colonel Sdrakas is the Subject Matter Expert in Electronic Warfare (EW), including Suppression of Enemy Air Defence (SEAD) Operations at the JAPCC.

An Operator's View on the Hypersonic Threat

Challenges and Imperatives for NATO

By Lieutenant Colonel Alfons Van Wuytswinkel, NLD Air and Space Force, JAPCC
By Colonel Kevin Anderson, US Air Force, JAPCC

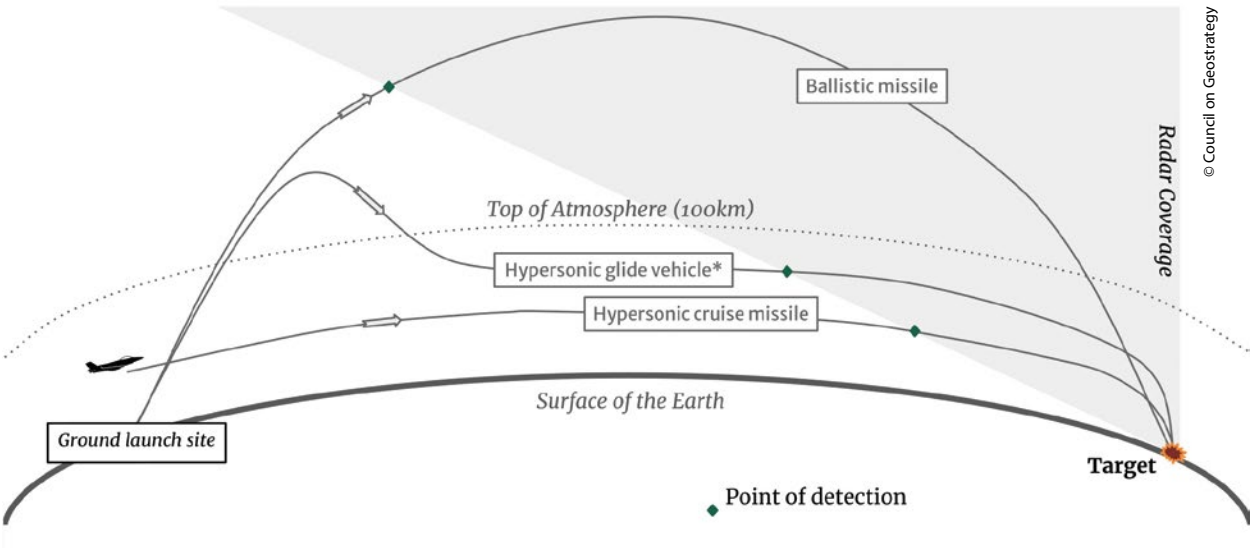
Introduction

"The responsiveness, manoeuvrability, and survivability of hypersonic weapons is unmatched by traditional strike capabilities for precision targeting, especially in anti-access/area denial (A2/AD) environments."[1]

This stark assessment by Lieutenant General Robert A. Rasch, the US Army's Rapid Capabilities and Critical Technologies Office director, describes a formidable challenge confronting NATO. Hypersonic weapons (hypersonics) are no longer a distant theoretical concern – they are here now, and potential adversaries, notably Russia and China, have actively developed and fielded these systems. Russia now routinely employs weapons like the Kinzhal and Tsirkon missiles in its ongoing war against Ukraine, providing a grim testament to the immediacy of this threat.[2,3,4,5]

To better understand the dilemmas created by these weapons, JAPCC is approaching the problem from the perspective of a Surface-Based Air and Missile Defence (SBAMD) operator. Here, at the human level, sitting at the critical juncture of technology, doctrine, and high-stakes decision-making, the new reality is particularly acute: existing SBAMD weapon systems, including the venerable Patriot system, were not designed to search, track, identify, and intercept threats that combine speeds exceeding Mach 5 with atmospheric manoeuvrability. Additionally, policy, doctrine, and training lag hypersonic development, creating gaps not only in defended airspace, but in strategic thinking as well.[6,7]

This article asserts that hypersonic weapons have reshaped the security landscape fundamentally, requiring a new category of defence integrated across multiple



Example hypersonic missile trajectories and radar coverage.

domains. Taking an operator's viewpoint, the article will characterize the hypersonic threat, detail the specific challenges confronting the SBAMD operator, examine the broader strategic deterrence implications, and provide recommendations for Alliance policy and capability development. The urgency is clear; understanding and addressing the hypersonic challenge, from the operator's console to the highest levels of strategic planning, is not merely prudent – it is imperative for maintaining credible deterrence and defence in the Euro-Atlantic area.

Hypersonic Missiles: More than Just Speed

For those unfamiliar with these weapons, understanding their characteristics is an essential first step. NATO defines hypersonic weapons as those which can sustain flight, and manoeuvre within the atmosphere, above Mach 5.[8,9] These characteristics allow hypersonic weapons to reach a potential opponent with speeds akin to ballistic missiles, and dynamic and unpredictable flight profiles that have no comparison.[10] The weapons primarily come in two variants, each presenting unique challenges:

- **Hypersonic Cruise Missiles (HCMs):** Like subsonic and supersonic cruise missiles, HCMs fly in a powered, non-ballistic trajectory. They are commonly powered by air-breathing engines, typically scramjets, enabling sustained hypersonic speeds within the atmosphere. One advantage of HCMs is that, due to their continuous propulsion, they can fly at low altitudes to complicate detection. One disadvantage is that they produce a large infrared (IR) signature due to their engines and skin friction heating. Russia's Tsirkon is a notable example of an HCM.[11,12]

- **Hypersonic Glide Vehicles (HGVs):** As its name implies, the HGV is a glide vehicle, typically launched with a large rocket booster which propels it to its desired altitude and speed. Once reaching the speed and altitude (typically 20–60km), the glide body separates and begins an unpowered, manoeuvring profile through the atmosphere, eventually diving towards its final target.[13] One advantage of HGVs is their smaller size and signature, while one disadvantage is they must start their profiles at high altitudes, wherein their initial launch may be more prone to detection than HCMs. Russia's Avangard, and China's DF-17 are both HGVs.

Challenges: The Operator's Crucible

While HCMs and HGVs have different design characteristics, they share common challenges for the SBAMD operator. They are hard to find, hard to track,

and even harder to intercept. The first challenge, therefore, is simply gathering the facts about the danger of these threats.

Although little information is available on intercept rates, in August 2024, Ukraine's armed forces claimed to have intercepted 30 out of 117 hypersonic missiles (25 %).[14] However, these numbers should be used with caution due to many 'known unknowns' such as the actual intercept rates of these weapons, Ukraine's defensive posture and coverage area, and the missile availability of their Patriot/SBAMD weapon systems. Additionally, some data may lead to false conclusions. For instance, Ukraine's notable success against Russia's Kinzhal must be put into context. While some reports indicate a high success rate in specific engagements, the Kinzhal is technically a ballistic missile with very limited manoeuvre capability; therefore, it does not represent a complete hypersonic challenge. Where there is reporting on the Tsirkon, a true HCM, the available data reflects a much lower intercept rate.[15,16]

While NATO awaits additional data, it can address other clear challenges, the 'known knowns' defying the operator. The unique characteristics of hypersonic weapons create profound difficulties for the operators of current SBAMD systems, spanning the entire engagement sequence. Some of these problems are listed below:

- **Detection and tracking difficulties:** Current ground-based radar systems face inherent limitations in detecting extremely fast, manoeuvrable targets which are potentially flying at low altitudes utilizing terrain masking. Unlike the high-altitudes of ballistic weapons, hypersonic flight profiles can create line-of-sight constraints which can delay initial detection, further compressing already short engagement timelines.[17,18]

- **Engagement geometry and interceptor limits:** Intercepting a hypersonic manoeuvring target is a daunting engineering problem. Interceptors must possess exceptional speed, extreme agility, and sophisticated sensors. Fortunately, the Patriot system has evolved significantly, with PAC-2 Guidance Enhanced Missile-Tactical (GEM-T) missiles optimized for ballistic missiles, and PAC-3 achieving hit-to-kill technology with additional attitude control motors (ACMs) to increase manoeuvrability. Nonetheless, sustained high-G manoeuvres of future hypersonics may exceed the kinematic capabilities of even the best interceptors.[19,20]

System Name (Designation)	Kinzhal (Kh-47M2)	Tsirkon (3M22)	Avangard	DF-17
Country	Russia	Russia	Russia	China
Type	Air-Launched Ballistic Missile	HCM	HGV	MRBM with HGV
Launch Platform	MiG-31K, Tu-22M3, SU-34	Ships, Submarines	ICBM (UR-100N, Sarmat), SS-19	Road-mobile TEL
Estimated Range	~2,000 km	~1,000 km	Intercontinental	~1,800–2,500 km
Reported Max Speed	Mach 4–10	> Mach 9	> Mach 27	Mach 5–10 (HGV)
Payload Capability	Conv/Nuc	Conv/Nuc	Nuclear	Conv/Nuc
Operational Status	Operational (Used)	Operational (Used)	Operational	Operational

Table: Lists of current hypersonic systems in Russia and China.

The DF-17 is reportedly capable of striking targets up to 2,500 km away and evading missile defence systems.

- **Decision dilemmas:** Having reflected on some of the technical challenges of hypersonics, questions for the operator remain: How do operators defend against this threat? Moreover, they must also ask not just 'how', but 'should we' attempt an intercept? Is the target (or potential target area) on the defended asset list (DAL)? Is the weapon payload conventional or nuclear? Do SBAMD batteries have suitable interceptors to engage? How many missiles should be shot at one target? Answering these questions is the 'defender's crucible' – with a short engagement timeline, they have mere seconds to verify, identify, prioritize, decide, and engage. The Observe, Orient, Decide, Act (OODA) loop has never been shorter.

Strategic and Deterrence Implications

Recognizing Alliance cohesion and public support as a strategic centre of gravity, NATO adversaries are expected to employ hypersonic weapons to achieve their strategic aims. Russia, for example, has demonstrated a willingness to attack cities to diminish public support for resistance. This directly amplifies the challenges for SBAMD operators, resulting in significant strategic and deterrence implications. Three specific strategic concerns are as follows:

1. **The unsustainability of comprehensive area defence:** Investing solely in defensive systems to intercept hypersonic missiles will not be sufficient to deter an opponent. The defender's cost burden is too high, both in terms of the number of missiles required and the overall coverage of radars and launchers needed across NATO.[21] In short, complete area defence is not an option due to prohibitive financial and logistic costs.

2. **Point defence vs the ambiguity trap:** Point defence is the strategy of electing to defend specific assets and areas within NATO territory. With this strategy, the quiet part is not typically said aloud,

but of course this implies deliberately letting weapons get through if they are not a factor to the DAL. Perhaps this is possible with conventional payloads, but the possibility of nuclear payloads may make this an unacceptable gamble. Additionally, manoeuvring hypersonics will create additional ambiguity for defenders attempting to determine the weapons' final impact points. [22,23]

3. **Erosion of strategic stability:** The introduction of hypersonic weapons creates a significant risk of miscalculation and escalation. Due to their ambiguous payloads and unclear trajectories, they blur the threshold between conventional and nuclear warfare. Furthermore, they may lead to 'first strike temptation', wherein the perceived ability to penetrate defences encourages both sides to attempt a 'left of launch' pre-emptive strike.

Collectively, these dilemmas mean NATO must rethink what a credible deterrence might involve. The next section provides recommendations on what this might look like.

Recommendations

NATO must consider what capabilities it needs to develop to counter the hypersonic weapon threat. Essentially, there are three options: mitigate the threat 'left of launch', intercept the threat 'right of launch', or accomplish a mix of both. The first option implies pre-emptively averting an enemy attack, potentially at the expense of escalation and miscalculation risks. The second implies a defensive posture which cannot be fully achieved.

Therefore, to be successful, a holistic Integrated Air and Missile Defence (IAMD) strategy should enable both offensive and defensive approaches. Fully interoperable systems must become the baseline, and Command and Control (C2) networks supported by adequate radar and IR sensor coverage must extend across the entirety of NATO airspace. Information dominance and cross-domain teamwork must become the new paradigm.

Furthermore, NATO must mirror hypersonic weapon dilemmas back on our adversaries by adding credible, perhaps the same, offensive capabilities to its inventory. Deep Precision Strike (DPS) capabilities must be reinvigorated. Possessing offensive weapons that can destroy the 'archers', not the 'arrows', imposes a strategic cost on our adversaries, who must expend significant resources on their own defence. Also, as part of a wider deterrent 'toolbox', these weapons create a dilemma for future opponents to deal with.

A robust offensive arsenal could achieve a new deterrence equilibrium that looks like the Mutual Assured Destruction (MAD)[24] theory from the Cold War. This

The US Patriot PAC-3 missile defence system, equipped with hit-to-kill technology and advanced Attitude Control Motors (ACMs), enhances manoeuvrability to intercept fast, agile targets – including emerging hypersonic missiles.

principle of deterrence is founded on prohibitive and credible escalation between parties. To achieve such credibility, NATO must do the following:

1. **Accelerate space-based sensing capabilities:** NATO must invest in space-based sensors which complement ground-based surveillance. This capability must include data-sharing agreements, common technical standards, and a robust C2 network to allow continuous tracking of hypersonic threats.

2. **Develop AI-supported decision tools:** To have a reasonable chance of successfully engaging hypersonics, a human operator must be aided by AI. Integration areas include data fusion, automated threat assessment, optimized engagement solutions, and a clear presentation of options to a human decision maker. Human-in-the-loop (HIL) and human-on-the-loop (HOL) paradigms have been thoroughly discussed in NATO, and SBAMD is an ideal use case for the emerging trend of incorporating AI into defence.[25,26]

3. **Accelerate NATO hypersonic procurement, testing, wargaming, and doctrine:** Working groups within the Alliance must work quickly to develop tactics, techniques, and procedures (TTP), Rules of Engagement (ROE), and C2 procedures to adequately prepare operators, intelligence analysts, and decision authorities for modern air defence realities.[27,28]

4. **Field 'left of launch' capabilities and enablers:** Nations should procure offensive capabilities supporting DPS, including hypersonic weapons, cruise missiles, and one-way attack (OWA) drones. Additionally, this hardware must be supported by robust intelligence gathering, cyber, and electronic warfare (EW) support, and other capabilities that can disrupt enemy launches, or support offensive operations against enemy launch platforms.

5. **Invest in resilient, interoperable, and distributed C2:** NATO C2 underwrites all SBAMD capabilities. It must be seamless, survivable, and redundant. Much has been written on the topic of NATO Air C2, but plans must be put into action within the decade.[29]

Conclusion

Should we shoot the arrow or the archer? It would be good to be able to shoot them all, and better still to not shoot any in the first place! Therefore, a new multi-domain deterrence approach is necessary. The emergence of operational hypersonic weapons presents a complex and urgent challenge to NATO's security. As operators on the front lines of NATO's air and missile defence will agree, these weapons stress current capabilities, compress decision timelines beyond human limits, and introduce dangerous ambiguities that can have strategic consequences.

The Alliance must adapt its defence strategies, considering whether current paradigms are sufficient for modern threats. This assessment must involve payload considerations, political and strategic risk, industrial capacity, and technical capabilities. Addressing this threat requires a comprehensive strategy that goes beyond simply trying to intercept incoming 'arrows', and instead focuses on disrupting the 'archer' before the shot, intercepting the 'arrow' if necessary, and fundamentally strengthening and shortening the air-defence OODA loop.

Doing so requires urgent and focused strategic thinking, collaborative policy development, and targeted investment in critical SBAMD enablers – particularly space-based sensing, AI-augmentation, C2 networks, and robust 'left of launch' capabilities. To successfully navigate the hypersonic era, NATO must overcome traditional stovepipes and implement an integrated, multi-domain approach adapted to its new security environment. ●

1. *US Department of Defense,* [website], 2024, https://www.defense.gov/News/Releases/Release/Article/3999835/army-and-navy-successfully-test-conventional-hypersonic-missile/, (accessed 3 March 2025).
2. Warren, S. A., *US Army War College,* [website], 2025, https://publications.armywarcollege.edu/News/Display/Article/4129339/russian-novel-nuclear-weapons-and-war-fighting-capabilities/, (accessed 25 March 2025).
3. Sayler, K. M., *US Congress,* [website], 2025, https://www.congress.gov/crs-product/R45811, (accessed 15 May 2025).
4. Shiffer, A., *JAPCC,* [website], 2023, https://www.japcc.org/articles/hypersonic-weapons-on-the-front-line/, (accessed 12 March 2025).
5. White, M, E., *Atlantic Council,* [website], 2025, https://www.atlanticcouncil.org/content-series/strategic-insights-memos/the-hypersonic-imperative/, (accessed 28 March 2025).
6. Toliver, B., *Global Security Review,* [website], 2025, https://globalsecurityreview.com/hypersonic-weapons-are-we-entering-a-new-era-of-vulnerability/ (accessed 31 May 2025).

7. Ramachandran, A., *ResearchGate,* [website], 2025, https://www.researchgate.net/publication/389689020_, (accessed 18 April 2025).
8. Brockmann, K. and Schiller, M., *Sipri,* [website], 2022, https://www.sipri.org/commentary/topical-backgrounder/2022/matter-speed-understanding-hypersonic-missile-systems, (accessed 15 March 2025).
9. Ibid. 3.
10. Watts, T. J. et al., *Atlantic Council,* [website], 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/08/Hypersonics-Weapons-Primer-Report.pdf, (accessed 10 April 2025).
11. Schmidt, A., *Army University Press,* [website], 2024, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-2024/Hypersonic-Capabilities/, (accessed 26 April 2025).
12. Ibid. 2.
13. Freer, W., *Council of Geostrategy,* [website], 2024, https://www.geostrategy.org.uk/research/britains-hypersonic-challenge-strategic-opportunities-and-risks/, (accessed 28 April 2025).
14. bne IntelliNews, 'Ukraine discloses for the first time real missile interception rates against the various kinds of Russian missiles', *bne IntelliNews, 24 August 2024,* https://www.intellinews.com/ukraine-discloses-for-the-first-time-real-missile-interception-rates-against-the-various-kinds-of-russian-missiles-340139/, (accessed 5 May 2025).
15. Ibid. 14.
16. Ibid. 2.
17. Shepard, J., *Sensor Tips,* [website], 2025, https://www.sensortips.com/featured/what-sensors-are-needed-to-counter-the-hypersonic-threat/, (accessed 15 April 2025).
18. Hollings, A., *Sandboxx,* [website], 2025, https://www.sandboxx.us/news/the-ultimate-guide-to-the-patriot-air-defense-system/, (accessed 18 March 2025).
19. Ibid. 11.
20. Ibid. 18.
21. Ibid. 11.
22. Johnson, M. D., *Missouri State University,* [website] 2024, https://bearworks.missouristate.edu/cgi/viewcontent.cgi?article=4987&context=theses, (accessed 27 March 2025).
23. Ibid. 6.
24. Britannica, [website], https://www.britannica.com/topic/mutual-assured-destruction, (accessed 23 March 2025).
25. Ibid. 7.
26. Daniels, O., *JAPCC,* [website], 2021, https://www.japcc.org/essays/speeding-up-the-ooda-loop-with-ai/, (accessed 25 March 2025).
27. Mehta, A., *DefenseNews,* [website], 2019, https://www.defensenews.com/industry/2019/03/19/northrop-launches-hypersonic-defense-push/, (accessed 12 February 2025).
28. Hill, D, J., US Senate Armed Service Committee Strategic Forces Subcommittee, [website], 2024, https://www.armed-services.senate.gov/download/hill-statement-050824?download=1, (accessed 23 March 2025).
29. Multinational Capability Development Campaign, [website], 2024, MCDC Multinational Multi-Domain Command and Control Interoperability, (accessed 23 April 2025).

ABOUT THE AUTHORS

Lieutenant Colonel Alfons Van Wuytswinkel
NLD Air and Space Force, JAPCC

Lieutenant Colonel Van Wuytswinkel has served for over 40 years in the Royal Netherlands armed forces and has completed several operational tours with the Netherlands Patriot unit in various positions.

He served in several command and training positions, in the realm of Surface-Based Air Defence and Missile Defence, as well as Internationally at the Competence Centre for Surface-Based Air and Missile Defence (CCSBAMD) in Ramstein, Germany. Before his current position he first served as Squadron commander and after that as Chief of Staff at the Netherlands GBAD command. Since June 2024 the author holds the Subject Matter Expert position for Surface-Based Air and Missile Defence at the Joint Air Power Competence Centre in Kalkar, Germany.

Colonel Kevin 'Tread' Anderson
US Air Force, JAPCC

Colonel Kevin 'Tread' Anderson is an F-16 instructor pilot, Wild Weasel, and Forward Air Controller (Airborne) with over 3,600 flight hours, 190 combat missions, and 1,000 combat hours.

His operational experience includes four deployments in support of overseas operations, as well as numerous NATO Air Policing taskings. Colonel Anderson commanded the 510th Fighter Squadron at Aviano Air Base, Italy. He is a graduate of the US Air Force Weapons Instructor Course, and holds master's degrees in Systems Engineering, International Relations, and Military Strategic Studies with an emphasis on joint planning.

Bridging the Gap

Civil-Military Cyber Cooperation After the NATO Summit in The Hague

By Pauline Malek, LLM, NLD National Cyber Security Centre and C2COE
By Stefan Nelwan, PhD, NLD National Cyber Security Centre and C2COE

Introduction

On the 24th and 25th of June 2025, The Netherlands hosted the NATO Summit in The Hague. During the run-up, the path to the NATO Summit was steep, with multiple geopolitical disruptions, from Russia's war against Ukraine, to asymmetric attacks on Allies, to the United States' shifting geopolitical focus from Europe. Yet the 2025 Summit was considered a great success, with NATO leaders agreeing to increase defence spending to 5 % of GDP annually by 2035. The NATO Summit also provided an opportunity to bolster the Netherlands' position as a dependable Ally as it was the first one hosted by Mark Rutte, a Dutch national and The Hague resident, since he was appointed the Secretary General of the Alliance. The target is to be split in two: 3.5 % on core military spending, and 1.5 % to defence-related investments such as cyber and resilience to hybrid threats.[1] With NATO and member states recognizing cyberspace as a warfighting domain, discussions about cyber in this context have increased within the armed forces. This includes the discussion on the impact for civil-military cyber collaboration, with a specific focus on improving the ways in which defence forces work with civilian partners to protect critical civilian infrastructure.

Despite the military preoccupation with the cyberspace domain, it is almost completely civilian run.

Executing Operation 'Orange Shield': The Netherlands Cyber Command was hard at work preparing for the 2025 NATO Summit.

In the Netherlands, the National Cyber Security Centre (NCSC-NL) leads civilian efforts, protecting and safeguarding Dutch networks and information systems. Its mandate includes functioning as a Computer Security Incident Response Team (CSIRT), advising service providers and central government organizations, assisting them, and conducting analyses and technical research.[2] Within the realm of cybersecurity, the military also has an important but more limited role. In the Netherlands, it conducts cyber operations under its own mandate, guided by constitutional tasks, the Intelligence and Security Services Act, and international law, including the Law of Armed Conflict (LOAC). The authors, operating in both the military and civilian capacities, acknowledge the need for civilian and military cooperation, but observe a gap in knowledge, mandates, and experience on both sides, undermining effective cyber threat deterrence.

Transformation of Cyber as a Warfighting Domain

Cyber has long been considered purely an Information Technology (IT) matter, even in military contexts, where it was primarily considered a supporting tool for traditional domains. However, geopolitical unrest and rapid technological progress have driven NATO's transformation, as reflected in the concept of Multi-Domain Operations (MDO), where cyberspace and space are now both recognized as warfighting domains. Across the Alliance, discussions increasingly focus on the question, *What does deterrence mean in the cyber domain?* This question, discussed mostly by strategic thinkers and lawyers rather than technical experts working in cyber, reflects a paradigm shift in which cyber is framed through the traditional lens of war planning and offers both advantage and vulnerability via kinetic and non-kinetic options.

Additionally, the cyber domain's expansion raises new questions about less visible adversaries and achieving military advantage in this space. These questions present challenges related not only to mandates and legal implications, but also to practical concerns like stakeholder cooperation and teamwork among skilled personnel. Moreover, civilian professionals are often unwilling to be sidelined by military decision makers, who, while skilled in strategy, may lack technical expertise and risk overlooking valuable civilian lessons.

Just as civil-military cooperation is codified with humanitarian organizations in conflict zones, a similar approach is needed with cyber. This requires moving beyond generalities of cyber warfare, which is too broad for meaningful cooperation, as it fails to grasp the complexity of the cybersecurity landscape or the diversity of threats posed by a wide range of actors and capabilities. Instead, a deeper conversation must lead to specific mandates and lines of authority between civil and military organizations, followed by deliberate training and exercises cementing procedures, roles, and crisis responses.

Challenges of Mandates and Authorities: Who is in the Lead?

Discussions within the armed forces regarding NATO's mandate often centre on Article 5 of the North Atlantic Treaty, which mandates a collective response to an armed attack. The narrative is that once this mandate is activated, NATO has a full range of military options at its disposal, relying on a deterrence doctrine built around its strong defence.

However, often overlooked is Article 5's grounding in international law, particularly Article 51 of the UN Charter,[3] which recognizes the right of a state to individual and collective self-defence, and that assistance occurs within the exercise of that right.[4] Little attention is given to NATO's obligation to report Article 5 actions to the UN Security Council, which has the authority to order a cessation of those actions.[5] Consequently, Article 5 is often cited incompletely, leading to the misconception that it alone provides a conduit for the use of force.[6] Geopolitical dynamics can complicate this process further, especially with key players like Russia and China being among the permanent members of the Council with the power to veto any resolution.

A further nuance exists with the concept of an 'armed attack' under Article 51 of the UN Charter, particularly the right of self-defence in modern hybrid warfare involving cyber threats. A cyberattack clearly classified as an armed attack in this sense would simplify the military defence mandate, including the use of force in the cyberspace domain. However, this authority still necessitates civilian cooperation, as private and public organizations largely control cyber infrastructure. Thus, purely military operations in cyberspace are non-existent, and questions remain regarding which responsibilities remain in civilian hands, and which actions fall within the military authority. While defence forces often assume they should take the lead, practical challenges arise.

In traditional discussions on the legitimacy of the use of force its legal framework, jus ad bellum, helps to make the conduct of operations more straightforward. However, there is concern that waiting for a similar cyberspace mandate is unviable, as purely academic discussions and outdated policies are unaffordable luxuries in real-world conflicts, as the war in Ukraine illustrates. It is complex to make a comparison between physical attacks and attacks within the cyberspace domain. What adds to the confusion is that the term 'cyberattack' is very common in the domain's day-to-day discourse and can be described as business-as-usual in civilian contexts. In discussions where terms such as 'hybrid warfare', 'information war' and 'cyberattacks' are freely used, how can we discern between attacks that surpass the threshold of traditional armed attack in the sense of Article 51 of the UN Charter, and those falling short of it? To illustrate an example, in the case of the 2022 cyberattack on Albania, which was attributed to Iran, NATO condemned it as a serious threat to the security of a member state.[7] It underscored NATO's view that cyberattacks could be potential triggers for invoking Article 5 of the North Atlantic Treaty, with the capacity to provoke collective action. Such attacks highlight the complexity of modern threats occurring in the grey zone and are seen to take place on a continuum of conflict, rather than binarily as war against peace.

It is therefore unwise to wait until a crisis to think about effective cyberspace deterrence. Today, state actors increasingly use hybrid attacks in peacetime, such as cyber and information warfare. Russia's cyberattacks against Ukraine challenge traditional armed attack notions, as these actions can cripple nations without physical violence, raising questions around attribution and accountability for cyber operations, especially when proxies are used. It is precisely in this peacetime grey zone where a clear framework is lacking, and without it, cooperation between Defence forces and other instruments of power falters.

Military in a Domain Run by Civilians

Unlike physical military operations, cyber operations face multiple constraints. Beyond its own network, the military enters an environment where nearly all infrastructure – networks, IT systems, and cloud services – is civilian owned. Freedom of movement often requires permissions, and civilian owners will prioritize business continuity, privacy laws, and regulatory requirements over military objectives.

NATO is often perceived as a defensive force, with deterrence and defence as core tasks. In conventional warfare, a show of force is an effective means of discouraging adversaries. However, in the cyberspace domain, this concept is problematic. First, protecting virtual assets is less visual compared to a physical military presence. Second, cyber forces are reluctant to reveal capabilities, as knowledge of

exploitable vulnerabilities provides a significant advantage in both offensive and defensive operations. Lastly, NATO has condemned malicious cyber activities aimed at undermining democratic institutions, national security, and society.[8] The Alliance promotes a free, open, peaceful, and secure cyberspace. Demonstrating destructive cyber capabilities may challenge the moral high ground.

In the cyberspace warfighting domain, LOAC applies during an armed conflict. Cyberattacks regarded as attacks within the meaning of LOAC can only be directed at military objectives. They must comply with the principles of distinction, proportionality, and precautions.[9] Military-led operations thus require clear rules of engagement to minimize collateral damage. However, limited intelligence and unknown interdependencies may lead to unintended consequences for civilian infrastructure. Effective situational awareness is vital, and civilian collaboration, while challenging, is essential. Additionally, military command structures are hierarchical, whereas civilian organizations span a wide spectrum of public and private stakeholders, some of whom may be unwilling to cooperate. Cyber assets, such as domain names, host IP-addresses, and digital content, may come from diverse sources, some of which are outside of the area of responsibility, reinforcing the need for an integrated cyber defence approach.

Opportunities for Cooperation: Cyber Crisis Management

ISO 22361 defines a crisis as an 'abnormal or extraordinary event or situation threatening an organization or community, requiring a strategic, adaptive, and timely response.'[10] Traditional crises, such as natural disasters or terrorism, are physical and visible, with clear public perception and hierarchical leadership responses.

Cyber crises differ significantly. In 2024, the European Union Agency for Cyber Security (ENISA) published a guide for managing cyber crises with a set of national best practices.[11] In the guide, they recognized the varied EU interpretations of cyber crises and recognized that a cyber incident can expand into a cyber crisis within milliseconds. Attribution is difficult, attack origins are remote, and interconnected systems can amplify attacks.

'It is precisely in this peacetime grey zone where a clear framework is lacking, and without it, cooperation between Defence forces and other instruments of power falters.'

© In Green/Shutterstock.com

To manage cyberattacks, many countries emphasize information exchange on vulnerabilities and threats. Effective exchange aids early detection, mitigation, or prevention of cyber incidents, increasing resilience and situational awareness. The effectiveness of this exchange depends on the specific needs of each organization. Coordinated responses among diverse entities, including law enforcement, national cybersecurity centres, intelligence agencies, and military units are essential. Military organizations, trained for crises, can contribute to MDO while benefiting from civilian collaboration.

Learning and Training Together

Joint exercises enhance mutual understanding between civilian and military organizations. They help train personnel, refine procedures, improve decision-making, and foster information sharing. Exercises in simulated environments, from table-top drills to wargaming and capture-the-flag events, sharpen individual technical skills and boost civil-military understanding.

Similarly, national-level exercises validate cyber crisis response. Many countries conduct such exercises, akin to drills for first responders, and notable examples include NATO's 'Locked Shields' and 'Cyber Coalition' from the NATO Collective Cyber Defence Centre of Excellence (CCDCOE), CyberEurope (ENISA), and ISIDOOR (NLD). ISIDOOR, named after the patron saint of the internet (St Isidore), is a biannual exercise conducted by the government of the Netherlands last held in 2023. In this fourth edition, over 120 organizations managed a fictitious vulnerability, and the exercise demonstrated the benefits of regular exercises.

Looking Back: The June 2025 NATO Summit

The Hague Summit was a high-profile event to emphasize the strategic importance of cyber preparedness and collaboration between organizations. In the lead-up to the Summit, the branches of the Dutch government and armed forces coordinated efforts to ensure national readiness and mitigate cyber threats associated with such an event. An example of civil-military cooperation emerged when the NCSC-NL requested operational support from organizations within the government and from the Ministry of Defence (MOD), leading to the deployment of cyber specialists to assist NCSC-NL.[12] This collaboration reflects the broader NATO strategic emphasis on 'whole of society' resilience and civil-military integration following the NATO Cyber Defence Pledge presented at the Vilnius Summit in 2023.[13] It reinforces that civil-military cooperation in the cyberspace domain is not merely useful, but essential to national and collective defence. The Dutch example shows that such cooperation is not only feasible, but can be operationalized effectively under real-world conditions if guided by shared objectives and trust.

For the strategy and investments that NATO envisages for 2035, further steps have to be taken. At this moment, there is a great divide between EU regulations and acts – meant for economic security in peacetime – and the principles of NATO, built on internal norms of collective security. This would be helpful in alignment on both on legislative and policy levels, for states to benefit from a shared vocabulary in NATO and EU documents when shaping their cyber strategies. Within the EU, member states must comply with obligations set out in EU directives and acts. These requirements should align with those established in NATO agreements, and vice versa. While NATO focuses on collective defence while the EU prioritizes economic cooperation, cyber activities must be harmonized to avoid confusion, particularly during a cyber crisis.

For instance, the Network and Information Security Directive 2 (NIS2) excludes defence and security actors from its scope, arguing that these matters fall under national jurisdiction. However, as Ministries of Defence often manage these systems, it is worth including them in national and Allied defence missions, increasing threat information sharing, and embracing cyber incident reporting duties.[14] The Netherlands MOD has submitted a bill for consultation for the Defence Readiness Act which provides powers with

regard to protecting and safeguarding Dutch networks and information systems of the MOD. In addition, the mentioned organizations are authorised to perform CERT-tasks and now would have the opportunity to become a military CERT and collaborate with civilian organizations, including NCSC-NL.[15] The authors are monitoring these developments closely, as they will affect the balance of the landscape, and therefore, the scope and form of civil-military cooperation in the cyberspace domain.

This last development indicates that the EU should assist Member States in implementing these regulations while ensuring NATO alignment. NATO documents, in turn, should reflect this perspective, helping Alliance members' defence sectors to establish a common understanding of incident-sharing responsibilities.

Implementing such an approach presents challenges, including NATO-imposed restrictions and varying national data-sharing interpretations. Therefore, Member State collaboration should not be limited to crisis response but should also include regular policy peer reviews. Proactive policy comparison and bold data-sharing decisions would enhance collective cyber resilience.

Post-Summit Observations: Towards Multi-stakeholder Coordination and Cooperation

The Summit also demonstrated that civil-military cooperation is far from a collaboration between two parties. From the civilian side, a wide array of organizations were involved, including national-level ministries, local government bodies, law enforcement agencies, and the Ministry of Justice and Security. On the military side, all branches of the armed forces contributed. The overall coordination effort was led by the National Coordinator for Counterterrorism and Security (NCTV), ensuring alignment not only in cyberspace but also in physical security domains. This multifaceted cooperation highlights the complexity of preparing for high-profile events and underscores the need for integrated planning across sectors.

Conclusion

Because civilian actors predominantly operate the cyber domain, civil-military cooperation is essential. Today's cyber threats remain deliberately below the threshold of armed conflict, requiring new approaches within existing legal frameworks. This challenges international law, as civilian actors – who are supposed to be protected in conflicts – are also the foremost experts in the cyberspace domain. Just as humanitarian organizations establish situational awareness and expertise in conflict zones before military forces arrive, a comparable rapport must be developed within the cyber community.

Continuous cyber threat response improvement requires collaboration between civilian and military entities. The authors emphasize the importance of joint learning efforts, and that their success lies in mutual, continuous learning and institutional memory. Defence agencies, governments, and industry leaders must therefore adopt a bold approach to information sharing and cooperation to strengthen cyber resilience and effectively combat cyber crises. Because cyber responsibilities span both civil and military sectors, new challenges will emerge. These issues should be addressed rather than avoided. The authors welcome ongoing initiatives and recognize that progress will involve difficulties, mistakes, and public debate, all of which are essential to refining cyber defence strategies.

The authors encourage leadership from all sectors to participate in cyber exercises, contributing their perspectives and expertise. While the cyber domain is complex on both technical and practical levels, exercises provide a controlled environment in which to assess solutions.

For the Netherlands, the NATO Summit in The Hague has offered a critical moment to demonstrate leadership in cyber crisis response. Highlighting both the urgency and the potential of civil-military collaboration and reaffirming its role as a key partner in crisis response within the Alliance. Before moving on to the next challenge, the authors propose using the NATO Summit as a catalyst to advance lasting civil-military cooperation in the cyber domain. ●

1. The Hague Summit Declaration, 2025, https://www.nato.int/cps/en/natohq/official_texts_236705.htm (accessed 10 August 2025).
2. The Netherlands, Network and Information Systems Security Act, Article 3.
3. Charter of the United Nations, Article 51.
4. North Atlantic Treaty, Article 5.
5. European Union Agency for Fundamental Rights, Official Journal of the European Union C 303/17, 2007, https://fra.europa.eu/en/eu-charter/article/51-field-application (accessed 10 August 2025).
6. North Atlantic Treaty Organization, 'Collective Defence and Article 5', 2023, https://www.nato.int/cps/en/natohq/topics_110496.htm (accessed 10 August 2025).
7. https://www.nato.int/cps/en/natohq/official_texts_207156.htm (accessed 10 August 2025).
8. North Atlantic Treaty Organization, 'Statement by the North Atlantic Council concerning malicious cyber activities against Germany and Czechia', 2024, https://www.nato.int/cps/en/natohq/official_texts_225229. (accessed 10 August 2025).
9. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 (AP I), Article 52 (2).
10. International Standards Organization, 'ISO 22361: 2025,2022', 2022, https://www.iso.org/standard/50267.html (accessed 10 August 2025).
11. European Union Agency for Cybersecurity, 'Best Practices for Cyber Crisis Management', 2024, https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management (accessed 10 August 2025).
12. https://magazines.defensie.nl/defensiekrant/2025/23/03_navo-top-cyberreservisten_23 (Dutch) (accessed 10 August 2025).
13. https://www.nato.int/cps/en/natohq/topics_78170.htm (accessed 10 August 2025).
14. European Commission, 'NIS2 Directive: new rules on cybersecurity of network and information systems', 2025, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (accessed 15 May 2025).
15. Bill for the Defense Readiness Act, in Dutch: https://www.internetconsultatie.nl/wet_op_de_defensiegereedheid/b1 (accessed 10 August 2025).

ABOUT THE AUTHORS

Pauline Malek

LLM, NLD National Cyber Security Centre and C2COE

Pauline Malek works as a Senior Legal Advisor at the Netherlands National Cyber Security Centre (NCSC-NL), and as a Visiting Expert at the NATO Command and Control Centre of Excellence (C2COE).

Previously, Pauline worked at the Clingendael Institute for International Relations, where she provided training for diplomats as well as military staff in the field of international law and security, and as a military legal advisor in the Royal Netherlands Air Force, where she advised on missions and operations.

Pauline started her career conducting research in the field of human rights law and the law of armed conflict, being based in Ghana, Bangladesh, and Palestine. Pauline serves as a reserve officer and holds an LL.M. in Public International Law from Leiden University, where she studied English Language and Culture. She speaks Polish, Dutch, English, German, French, and Russian.

Stefan Nelwan

PhD, NLD National Cyber Security Centre and C2COE

Stefan Nelwan works as a Team Manager, leading the Crisis Preparation Unit at the Netherlands National Cyber Security Centre (NCSC-NL), and at the NATO Command and Control Centre of Excellence (C2COE). At NCSC-NL, his focus is on the preparation, management, and evaluation of cyber crises, and the organization of the largest joint cybersecurity exercise in The Netherlands. At the NATO C2COE Stefan serves as a Staff Officer, where his research interests include civilian and military cooperation, human factors, leadership, and team performance for resilient and effective crisis response. Previously, Stefan worked at the Erasmus University Medical Centre as a Manager Medical Technology and scientific researcher. He holds an MSc. in Medical Informatics from Erasmus University, as well as a Ph.D. in Signal Processing, in which he worked on new patient monitoring methods in the field of cardiology and epidemiology.

Forging Adaptive Leaders for NATO's Space Frontier

By Captain Maria Soto, US Air Force, USSPACEFOREUR-AF

Introduction

Following NATO's 2019 declaration of space as an operational domain, many Allies have advanced their national military space programmes and integrated these capabilities into their Alliance contributions. Space differs significantly from terrestrial domains, which have established doctrines and deep operational experience. Instead, it is characterized by rapid technological evolution, prevalent dual-use technologies, a growing reliance on commercial vendors, and an evolving, often ambiguous, legal framework. Furthermore, with key NATO organizations like the Space Centre of Excellence (COE) and Combined Force Space Component Command (CFSpCC) still maturing and Tactics, Techniques, and Procedures (TTPs) in constant evolution, the Alliance operates in a domain where doctrine is being written in real-time.

Operations in this domain are not conducted independently, but in support of all others, with effects generated by operators who are physically separated from both the battlefield and the orbiting assets they control. This dynamic environment, combined with inconsistent organizational structures–where some nations have dedicated military space commands while others integrate professionals into traditional air force structures–highlights a pressing challenge: cultivating a new generation of military leaders. The choices these leaders make will be paramount, often occurring with incomplete information and under immense pressure. To prevail in these complex conditions, NATO's space leaders must be deliberately trained through a new paradigm focused on cognitive agility, innovation, and resilience to master the ultimate high ground.

© Ministère des Armées (@Armees_Gouv)/X

Multinational exercises like France's AsterX, aim to foster innovation, cooperation, and interoperability alongside industry partners in the space domain.

The Three Pillars of Modern Space Leadership

The evolving character of warfare requires military leaders to be competent across multiple domains, with adaptability in complex environments. Because space is uniquely intertwined with other domains, leadership becomes a 'complex, multipath process' rather than the 'single, top-down construct' most domains are accustomed to.[1] This necessitates a leadership development paradigm tailored to the distinct demands of NATO's space missions, focusing on three pillars.

The first pillar is *cognitive agility,* the capacity to rapidly analyse complex, often incomplete, space situational awareness data; to mentally flex and adapt plans in response to dynamic threats; and to make sound, timely decisions under pressure amid ambiguous rules of engagement. The complexity of the space environment needs to be cultivated in leaders to balance this risk of uncertainty with the responsibility of command. This requires leaders who can think critically, anticipate second- and third-order effects, and comfortably navigate uncertainty.

Next, this agile mindset must be paired with a drive for *innovation,* the need for creative solutions inherent to progress in a developing field. It means fostering and implementing novel operational concepts, integrating inventive technological applications (often from commercial partners), and championing process improvements to enhance NATO's space capabilities. As leadership is the lynchpin guiding organizations through change, commanders must encourage creative problem-solving without fear of failure, recognizing that the consequences of inaction often outweigh those of action.[2]

Finally, underpinning both agility and innovation is *resilience,* the foundation for sustained operations in a demanding, contested domain. It is the capacity to maintain leadership, team cohesion, and mission focus during and after disruptions to space capabilities, whether from adversary action, technical malfunction, or environmental factors. Resilient leaders foster an environment where subordinates persevere

through ambiguity, adapt to changing circumstances, and bounce back from adversity. This involves building trust, managing stress effectively, and possessing a keen awareness of their own limitations and abilities, trusting that where they have weaknesses, others will have compensating talents.

'As leadership is the lynchpin guiding organizations through change, commanders must encourage creative problem-solving without fear of failure, recognizing that the consequences of inaction often outweigh those of action.'

The complexities of the space domain require leaders who can balance the inherent risk of uncertainty with the responsibility of command. While foundational leadership principles remain relevant, their application in the unique space context requires dedicated adaptation. Traditional military leadership development relies on tactical ground or air manoeuvres – opportunities less available to space officers. Therefore, NATO must forge new pathways to instil these essential qualities.

Cultivating Adaptive Space Leaders: Innovative Approaches for NATO

The relative novelty of the space domain offers NATO a unique opportunity to intentionally design an educational framework that meets modern needs. The Space COE, CFSpCC, Allied Command Transformation (ACT), and the NATO School Oberammergau (NSO) are all stakeholders in developing quality education for future NATO space leaders. Some NSO courses increase space domain IQ, but NATO currently offers no programs that combine this knowledge with space leadership development. As the COE develops its own courses, focus on unique leadership skills would set them apart while augmenting NSO space courses. Since these courses are in development, incorporating these leadership development proposals as a central focus would pay dividends to the calibre of space leaders that NATO produces.

Leverage External Expertise to Build Best Practices

Space education should leverage guest speakers from industry and national space agencies from NATO Allies. Like the cyber domain, the space domain relies heavily on commercial equities. Technological advances are enhancing space capabilities, and 'partnerships between military, industrial, and academic entities are lighting the way to new innovations in dozens of mission areas.'[3] Learning from real-world experiences instead of textbook responses provides a dynamic, relatable experience that learners can internalize for future situations. Seminars with industry panellists can provide a platform to explore leadership development assumptions among stakeholders and influence what military leaders prioritize. Additionally, the commercial industry has effectively embraced a culture of learning from failures in the space domain. Sharing these lessons learned with a military culture averse to failure may foster innovative strategies for space operations.

To enhance agility, the NATO vision for space should prioritize training courses but also provide opportunities outside of traditional education for space professionals in dedicated NATO billets. Partnering with existing NATO organizations like the Defence Innovation Accelerator for the North Atlantic (DIANA) can strengthen innovation and industry relationships for space leaders. DIANA could pose current challenges as part of a space capstone course for students with various backgrounds to work through. Even if no viable solutions are discovered, it still presents current, real-world challenges to educational forums. Leadership forums focused on innovation and industry may help discover creative ways to tackle issues that leaders cannot solve individually.

Foster a Joint, Combined, and Multi-Domain Mindset

As space becomes a distinct career field in many Allied nations, 'few Space officers will have the experience of leading troops, so the culture will likely evolve to one of officers as highly skilled technicians rather than as leaders'.[4] Additionally, space operations are not conducted in isolation; they overwhelmingly support

terrestrial domains. Even the US Space Force Spacepower Doctrine 1-1 acknowledges that 'space power cannot unilaterally win wars.'[5] To succeed in NATO roles, space leaders must understand how other domains leverage space capabilities in their operations. As these officers progress into operational and strategic levels within the Joint Force, many will struggle to integrate effectively due to limited leadership experience and Joint exposure.

Recognizing space as an enabler highlights the need for cross-domain understanding and collaboration, rather than isolated development within stovepiped services. In the joint environment, NATO must develop space leaders more holistically to produce adaptive, creative contributors to the fight.[6] While education is critical, it must be balanced against limited operational manning. Courses should prioritize tactical depth and operational leadership, remain current with space advancements, and minimize time away from mission roles. Space Coordination Elements (SpCE) provide subject matter expertise to AIRCOM, LANDCOM, MARCOM, and JFCs, educating them on space capabilities. Expanding space education across other domains would help all branches better understand how space supports terrestrial warfare, and help space officers better grasp how their domain integrates with air, land, sea, and cyber operations.

To relieve pressure on NATO JFCs, dedicated leadership development and joint-focused space education programs are needed. Space courses must move beyond domain-specific instruction and prepare officers for integrated joint operations.

Beyond the Science: Cultivating the Art of Leadership

Leadership is often touted as 'an art and a science.' Space professionals must master both 'space domain knowledge' and 'unique operational art' to accomplish objectives and collaborate with other space-oriented partners.[7] Current space education emphasizes the science and technical aspects throughout NATO and national military courses but lacks in developing the *art* aspect of leadership and the applied skills of a space leader. 'Successful leaders are able to balance emotional quotient (EQ) and IQ to lead in the technical environment in which Space operates.'[8] Focusing course material on these skills alongside space knowledge will develop more well-rounded individuals contributing to NATO.

'To succeed in NATO roles, space leaders must understand how other domains leverage space capabilities in their operations.'

One of the most critical skills for emotional resiliency is developing a 'meta-view' or 'view from above.'[9] Fitting the space vision, leaders can utilize this skill to broaden perspectives and develop personal growth through reflection on mistakes. To develop this self-awareness, 360-degree feedback can be incorporated into leadership development. This compares an individual's self-perception with how their peers, subordinates, and leadership see their skills. Individualized coaching can then be provided to improve the delta between perceived strengths and weaknesses. Also, demonstrating how one's areas of weakness can be balanced with another's strengths develops a team mentality.

Bridging the Space Leadership Gap Through Tailored Education & Training

There is a lack of tactical-level space exercises through which junior officers can learn leadership skills. Due to this, 'many of the members are technologically smart but lack self-awareness skills that leaders need to foster cohesive teams.'[10] The growing complexity, met with limited leadership experience, creates a development gap for space officers. The challenge for educators is to develop leaders that can adapt rapidly to change and thrive in the uncertainty of social complexity, technological advancements, and globalization.[11] Developing these skills requires a great deal of time and resources, which NATO currently lacks, especially in the space domain.

The connection between successful leadership in complex adaptive environments and Emotional Intelligence

© NATO_ACT

Fifteen of the thirty-two NATO nations currently sponsor the NATO Space Centre of Excellence.

(EI) is well-established by research. EI incorporates traits of self-awareness, empathy, and relationship-building, which help leaders rely on their team and improve operational agility. In effect, EI distinguishes great leaders from average ones by the ability to make people feel more capable, inspired, and supported. In the ambiguous space environment, where rules of engagement are unclear, creating this environment of trust is vital to decrease the time it takes to vet and negotiate decisions. Training leaders to build this trust is challenging but valuable for teams postured to respond to unknown tactics.

NATO ACT's Layered Resilience Concept provides a comprehensive framework for this training. The central idea is that resilience is a multi-layered capability requiring a holistic approach to withstand, adapt to, and recover from unforeseen interferences. Recognizing that modern threats are often complex and interconnected, this framework can be translated into practical training for space leaders. This training would focus on stress resilience, psychological preparedness for degraded or denied space environments, and team leadership during crises.

A Flagship Proposal: A NATO Space Warfighter Program

To address the gap in tactical leadership experience and tie these developmental concepts together, NATO should establish a dedicated *Space Warfighter Program (SWP)*. Inspired by models like the US Air Force Weapons Instructor Course, the SWP would be an advanced, intensive course focused on creating deep technical and tactical experts in NATO space operations. This program would serve as the ideal vehicle to implement the pathways described above. Its curriculum would be built on a foundation of EI and the ACT Layered Resilience Concept, challenging students with high-stakes crisis scenarios. It would integrate industry partners and Joint Force planners

directly into the training, and its graduates would form a cadre of NATO Weapons Officer equivalents, space–elite integrators capable of developing and disseminating advanced TTPs across the Alliance, significantly enhancing NATO's operational edge.

Conclusion

The unique challenges of the space domain demand that agile, innovative, and resilient professionals are ready to support joint operations. These traits must be deliberately cultivated, as the domain does not offer the same tactical command opportunities available to junior officers in the terrestrial domains. Stakeholders in NATO's space enterprise have the advantage of creating new developmental resources without the constraints of pre-existing structures. The challenge, therefore, is to translate these essential leadership traits into tangible education, exercises, and experiences.

The path forward requires incorporating industry expertise to drive innovation, increasing the Joint Force understanding of space integration, and emphasizing the 'art' of leadership in a technology-dominant field. A dedicated *SWP* represents the most effective and direct way to achieve this, creating a cadre of expert leaders who can master the complexities of the domain. Failure to deliberately forge these leaders is not an option. It would leave NATO's warfighters in all domains vulnerable and cede the advantage on the ultimate high ground to our adversaries. The time to build the next generation of NATO space leadership is now. ●

1. D. Watkins, M. Earnhardt, L. Pittenger, et al, 'Thriving in complexity: A framework for leadership education' Journal of Leadership Education, 148–163, 2017, https://doi.org/10.12806/V16/I4/T4 (accessed 9 July 2025).
2. C. Gehler, 'Agile Leaders, Agile Institutions: Educating Adaptive and Innovative Leaders for Today and Tomorrow', 2005, https://apps.dtic.mil/sti/pdfs/ADA434868.pdf (accessed 9 July 2025).
3. D. Roberson, M. Stafford, 'The Redesigned Air Force Continuum of Learning: Rethinking Force Development for the Future', Air University Press, 2017.
4. M. Soto, 'A Qualitative Analysis into Space Force Leadership Development (Doctoral Thesis)', University of Arizona, 2024.
5. J. W. Raymond, 'Chief of Space Operations' Planning Guidance', Center for International and Strategic Studies, 2020, https://aerospace.csis.org/wp-content/uploads/2020/11/CSO-PLANNING-GUIDANCE-compressed.pdf (accessed 9 July 2025).
6. Ibid.
7. Ibid. 5.
8. Ibid. 5.
9. S. David, 'Emotional Agility: Get Unstuck, Embrace Change, and Thrive in Work and Life', Penguin House Publishing, 2017.
10. Ibid. 9.
11. Ibid. 9.

ABOUT THE AUTHOR

Captain Maria Soto

US Air Force, USSPACEFOREUR-AF

Captain Maria Soto enlisted in 2010 as an Emergency Management specialist and commissioned into the Space Operations career field in 2021. She has a background in Space Electromagnetic Warfare and currently works in the International Affairs Division of US Space Forces in Europe & Africa (USSPACEFOREUR-AF).

Capt Soto's diverse background includes a deployment to Ali Al Salem Air Base, Kuwait in support of Operation ENDURING FREEDOM; exercise planning for USNORTHCOM, USEUCOM and NATO Tier 1 exercises; and planning Security Cooperation engagements with the Republic of Slovenia and the Hashemite Kingdom of Jordan through the Colorado State Partnership Program. Her educational background includes a Bachelor's Degree in Philosophy and Political Science, a Master's Degree in Emergency Management, and a PhD in Organizational Development and Leadership.

Train, Adapt, Repeat

How AI is Reinventing Air Control Instruction

By Bernd Velling, Battle Management Analyst, Vectrona

Introduction

Competent air controllers are essential for effective air power, especially as global security deteriorates and air battle management becomes more complex. However, the training process has several challenges, both in training structure and personnel management.[1] Modern air operations involve rapid information flow and sophisticated threats, meaning training methods must keep up. This paper examines these challenges, with a focus on air battle manager (ABM) training. It also explores how artificial intelligence (AI)-driven support systems can help improve traditional training, benefiting both students and instructors. Challenges inherent in international training environments, such as cultural, language, and logistical differences, underscore the need for more adaptive and reliable training solutions.

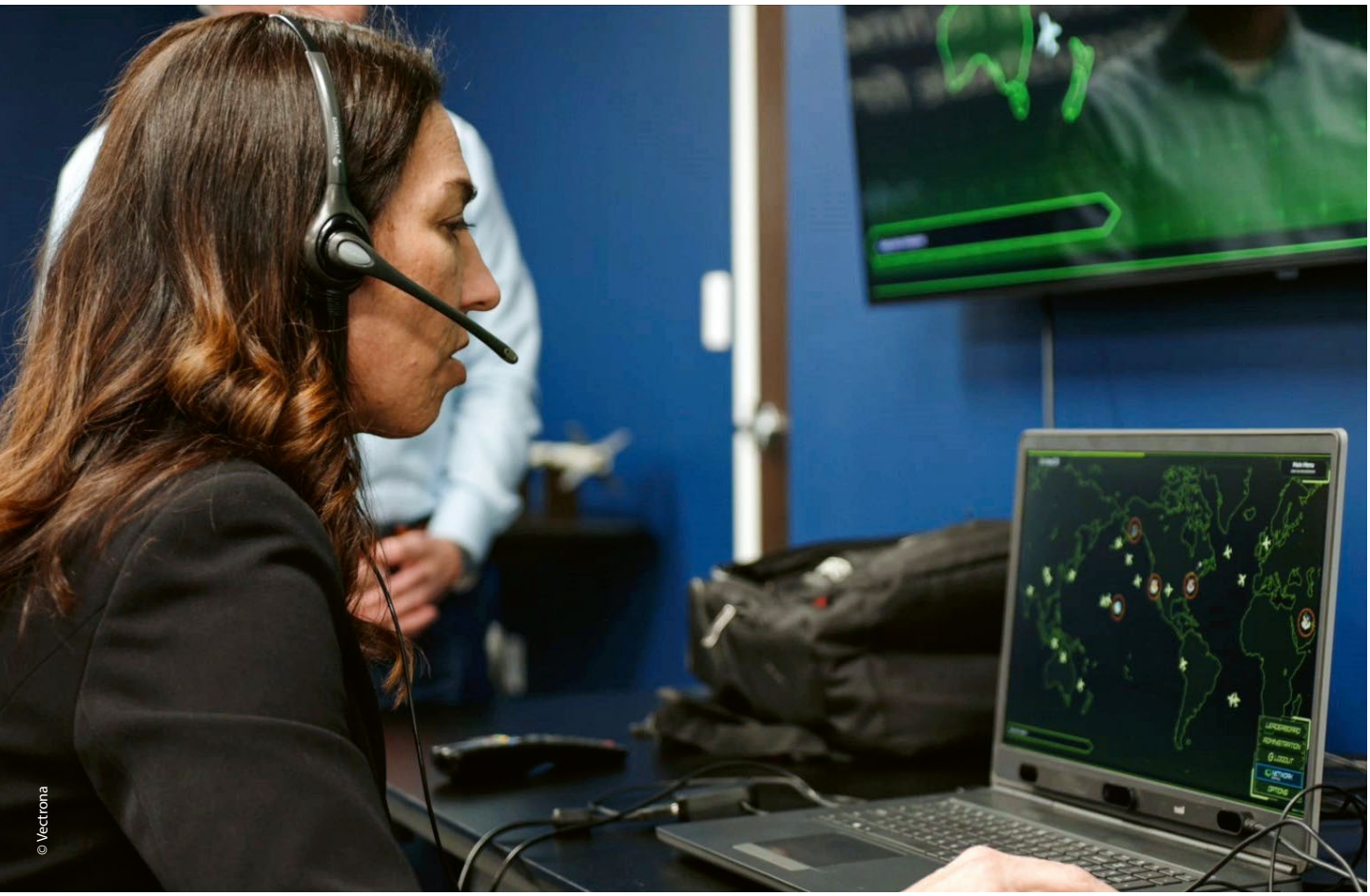
This analysis will first outline what an effective training framework looks like. Then, it will examine common problems, such as system failures and insufficient resources. After that, it will introduce and evaluate an AI-driven training solution, looking at its technical characteristics, why it works from a teaching perspective, and its practical benefits. The discussion will use historical examples and recent case studies. Finally, the conclusion will emphasize that AI-supported ABM training is a viable and effective means to support, but not replace, human instructors, helping to create a stronger and more efficient training program.

'AI-driven systems do not replace instructors – they free them to focus on what only humans can do: mentor, adapt, and lead.'

The Landscape of Air Controller Training: Frameworks and Fissures

A sound training system for air controllers needs clear goals, defined prerequisite skills, and organized timelines. It also needs objective standards for judging student performance.[2] While designing a whole program is a big topic, this analysis focuses on the basic '101 level' of air controller training.

The support needed for this kind of training is significant. It includes dedicated courses, qualified instructors,



Controllers conduct a simulated mission at the Vectrona testing facility, leveraging AI-driven command and control training tools.

advanced simulators (and the technicians to run them), training facilities, and extensive information technology (IT) systems. The reliability of all this is key, but it is often a weak point. Still, the people – instructors and support staff – are the real backbone of these operations. Most air control training programs are currently split into academic, simulation, and live training phases. These often happen in order, with classroom learning before practical exercises, but this can change based on the course and the student's background. For example, there are faster options for experienced personnel.

Even with careful planning, training systems, especially complex simulators, can face severe disruptions. Hardware or software failures, which can sometimes affect multiple connected systems, can cause long delays and create scheduling headaches, even if backup systems are in place. Upgrades or major maintenance work can also reduce simulator availability, often clashing with existing training schedules and affecting how quickly groups of students can progress. Sometimes, simulators are in different buildings, making access difficult, depending on whether the system is working and if an instructor is available.

The Human Element: Instructor Burden and Resource Allocation

A common problem in military training is that there are often too many students for each instructor due to limitations within the organization. Instructors frequently have many duties beyond just teaching, such as administrative work, developing course materials, scheduling, and keeping up their own operational qualifications.[3] Juggling all these tasks can be very demanding. In multinational units, these problems are even bigger. International students might need extra help with language, adjusting to different teaching styles, adapting to a new culture, and making practical arrangements. They often turn to instructors for this help, which takes away time from core teaching duties and gives individual attention to students.

While instructors usually accept these extra duties as part of the job, splitting their time inevitably means less time for preparing and delivering training, which is problematic when it comes to repetition-based learning environments like ABM training.[4] No matter how basic, every training exercise needs an instructor, a simulator, and simulator operators. When this practice is interrupted – because of system problems, an unavailable instructor, or scheduling conflicts – students can go for long periods without practical experience. These gaps are particularly hard on less experienced trainees, especially those working in a language that is not their own. This can lead to skills fading, feeling overwhelmed in high-pressure live situations, and, in the worst cases, failing missions or dropping out of training. The resulting instructor fatigue and burnout can also lower the overall quality and effectiveness of the training program.

AI-Driven Training Systems: A Scalable Solution

To tackle these many challenges, NATO needs scalable solutions that directly help students learn while reducing the load on instructors. One promising idea is using laptop-based, AI-driven training platforms that can work with any Command and Control (C2) system.

System Architecture and Capabilities: Such a system, which can be considered an interactive simulator, lets student controllers practice basic air control scenarios (like simple two versus two non-manoeuvring engagements) independently. The teaching approach is a mix of machine learning (ML) and other AI techniques. Key parts include:

- **Intelligent Tutoring System (ITS):** The ITS gives real-time, relevant feedback while running a scenario. This feedback can appear as text on the screen or as a synthesized voice, using different ways to help students learn. An ITS usually includes a domain model (with expert knowledge of air control procedures), a student model (which tracks individual progress, common mistakes, and likely knowledge gaps based on performance), and a pedagogical model (which decides the best way and time to offer help).[5] How well the pedagogical model works is key to making sure feedback is helpful and not excessive.

The author demonstrates the C2 training system during a field exercise, after which the students proceeded to train independently on their own systems.

- **Adaptive Difficulty Engine:** ML algorithms can change how complex a scenario is in real time based on how the student is doing. This ensures the challenge keeps the student in their 'zone of proximal development'.[6] This might mean changing the number of aircraft, how they move, weather conditions, communication demands, or adding unexpected events, all of which help students become more adaptable and better problem-solvers.

- **Multimodal Input and Cognitive State Assessment:** Using eye-tracking technology allows the system to monitor where students look (such as their scan patterns and how long they look at certain things) and physical signs of mental effort, like pupil dilation. Combined with voice analysis (e.g. speech rate, hesitations, and clarity) through speech-interactive avatars, the system can assess a student's stress and cognitive overload levels, prompting assistance from the ITS or changes to the scenario's difficulty.

- **Portability and Accessibility:** Because the system runs on regular laptops with standard equipment like headsets and footswitches, training can happen in many places – classrooms, remote locations, or even at home. Cloud-based user profiles help track progress and let instructors see student performance data remotely, allowing for more specific feedback and support, and creating a more continuous learning experience.

As to educational rationale and benefits, adaptive and AI-driven learning approaches work based on well-known learning principles. When students can practice deliberately, repeating scenarios at their own speed, they develop automatic skills and muscle memory for complex procedures.[7] The immediate, personalized feedback from the ITS fits with ideas of active learning and learning from mistakes, helping students understand and correct errors faster. By delegating basic, repetitive tasks, instructors can use their expertise for more complex scenarios, one-on-one mentoring, and advanced teaching. Also, because basic air control procedures are unclassified, scenarios can be run in a 'mission-unspecified' way, avoiding security issues tied to classified simulators.

Empirical Support and Case Study Analysis

The potential benefits of these AI-supported systems are not only theoretical. Past training disruptions and recent evaluations provide strong evidence.

Two training systems deployed to an austere environment demonstrate operational readiness during the exercise.

- **Operation Allied Force (Kosovo, 1999):** When NATO halted basic AWACS controller training for a month due to operational needs, it created a huge training backlog that took almost two years to clear. An accessible, AI-driven system could have let student controllers keep practicing and improving their procedural skills during this time, reducing the backlog. For example, if students had about six hours of training per day, they could have accomplished around thirty AI-driven missions per day. Over twenty duty days (four weeks), that is six hundred missions, helping them maintain necessary learning momentum.

- **NATO AWACS Midterm Upgrade (2006–2008):** The major system changes during this fleet upgrade suddenly created separate training paths and a need to retrain existing personnel, overwhelming simulator availability and instructor resources. A portable AI system could have offered a flexible way to practice standard procedures relevant to the old and new systems. It could also have helped new students learn basic control concepts before approaching high-demand simulators.

- **Air National Guard (ANG) Evaluation (2022):** A competition involving ANG Battle Control Centres used an AI-supported system as a case study. Airmen controlled 336 missions, getting 65 man-hours of training value. Achieving the same training output with a standard simulator and its support staff would likely have taken an estimated 756 man-hours. This data suggests a potential twelve-fold increase in training efficiency for the scenarios tested. It highlights significant potential cost-savings in man-hours and the ability to train more people.

These examples show how AI-driven systems can help keep training going during disruptions, manage sudden increases in training demand, and make better use of training resources.

Discussion and Future Directions

Using AI-driven training systems represents a significant shift in tackling long-standing air controller training problems. The main benefit is in supporting human instructors, not replacing them. These systems can make quality procedural practice more widely available, reduce instructor burnout from repetitive basic tasks, and provide rich data for tracking student progress and finding areas where training could be improved.

However, putting these systems into place does have its challenges. Developing AI models that are effective training aids requires a lot of upfront investment in expertise and testing.[8] It is vital to ensure that AI-generated feedback helps students perform better in complex, real-world situations. Various ethical concerns must be mitigated, especially around data privacy and the chance of AI assessment bias. Future research should continue to examine AI's effectiveness in training and explore how training aids can be combined with live missions and high-fidelity simulation training. Additionally, there is work to be done to create more advanced, adaptive scenarios that enhance complex thinking skills like high-pressure decision-making and crewmember teamwork. As a potential avenue of future work, JAPCC might explore how AI can be used to develop more complex teams and multi-agency collaborations.

Conclusion

AI-driven training solutions, like portable, adaptive platforms with ITS features, offer a powerful way to make air controller training programs more efficient, accessible, and robust. By allowing self-directed, repetitive practice in a controlled setting, these systems can improve student results, lessen instructor workload, and ensure training can continue even with logistical or resource problems. For organizations that want to stay at the forefront of air power, using these kinds of technological innovations is not just helpful – it is becoming essential for preparing controllers for the complexities of modern operations. ●

1. Smith, J, Q., Jones, M, R., and Brown, C, D., 'Advancing Managerial Evolution and Resource Management in Contemporary Business Landscapes', *Journal of Management Studies,* vol. 58, 2020, pp. 1–25.
2. Bell, H., and Reigeluth, C, M., 'Paradigm Change in Military Education and Training', *Educational Technology,* vol. 54, 2014, pp.52–57.
3. Dr Hasan, A, H., and M. Naser, M., 'Teaching Challenges in a Military Setting', *Australian Journal of basic and applied sciences,* vol. 7, no. 7, 2013, pp.161–166.
4. Ericsson, K. A., Krampe, R. T., & Tesch-Römer, C., 'The role of deliberate practice in the acquisition of expert performance'. *Psychological Review,* vol. 100, no. 3, 1993, 363–406.
5. Nkambou, R., Mizoguchi, R., and Bourdeau, J., *Advances in Intelligent Tutoring Systems,* Heidelberg, Springer Berlin, 2010.
6. Vygotsky, L. S., *Mind in society: The development of higher psychological processes,* Cambridge, Harvard University Press, 1978.
7. Atkinson, R. C., and Shiffrin, R. M., *Human memory: A proposed system and its control processes,* in K. W. Spence and J. T., *The psychology of learning and motivation.* Academic Press, vol. 2, 1968, pp. 89–195.
8. Polson, M. C., and Richardson, J. J., *Foundations of intelligent tutoring systems,* New York, Psychology Press, 1988.

ABOUT THE AUTHOR

Bernd Velling

Battle Management Analyst, Vectrona

Bernd Velling is a retired Senior Master Sergeant who served over 35 years in the German Air Force. Bernd spent 33 years in different NATO assignments, 22 of which were as an aircrew member on NATO AWACS, accumulating more than 7,000 hours flying missions spanning the range from UN missions supporting operations in Former Yugoslavia including Operation Allied Force, post-9/11 counter-terror missions, and deployments to Afghanistan under the ISAF mandate. Of his 22 years as active aircrew, he spent more than 17 years in instructor, evaluator, and training development positions. A communications specialist by trade, he quickly grasped the overall importance of a holistic mission view and training as the backbone of any operation. He lives in the US and works for Vectrona.

Wargaming in Future Force Design

Unlocking Operational Art in the Process

By Lieutenant Colonel Dr Gwendolyn Bakx, NLD Air and Space Force, JAPCC
By Mr Antoine de Reus, Royal Netherlands Aerospace Centre

Introduction

During World War II, members of the Women's Royal Naval Service (Wrens) developed a remarkably effective wargame to counter German U-boats.[1] Armed with little more than chalk, bedsheets, and a basic understanding of naval warfare, they simulated convoy movements and enemy submarine attacks, enabling naval officers to refine their anti-submarine strategies.[2] This simple yet powerful exercise led to new tactics, techniques, and procedures (TTPs) and dramatically improved the Royal Navy's ability to protect vital supply lines in the Atlantic.

This historical episode underscores wargaming's enduring value – not only in tactical applications, as seen in the Wrens' story, but also in shaping NATO's modern capabilities. NATO now navigates an era of escalating global competition, proxy warfare, technological disruption, and multi-domain conflict.[3] Much like in World War II, decision makers must contend with uncertainty and complexity in this volatile security landscape. In response, NATO has renewed its emphasis on wargaming as a vital analytical tool to drive transformation by strengthening underlying conceptual foundations.[4]

A Need for Deliberation

Recent advancements in the air and space domains reflect wargaming's growing role in formulating and evaluating concepts for future force design.[5] Consequently, this edition of the JAPCC Journal presents a timely opportunity to explore wargaming's broader dimensions and strategic implications in this evolving context.

This article posits that wargaming is an indispensable instrument for concept development in future force design. Primarily, because wargaming – with its human-centric nature – has the power to sharpen strategic thinking and cultivate operational art into this process, i.e., to conceptualize future force requirements in ways that transcend computational logic. However, policymakers and military leaders must avoid misguided conclusions or unrealistic expectations to leverage its strengths in future force design efforts effectively. This requires recognizing the intrinsic analytical limitations of wargaming within this process. While science plays a crucial role in shaping future forces, wargaming's core value is that it fosters operational art: it enhances the participants' critical thinking, stimulates their imagination, and helps them gain conceptual clarity in complex and uncertain scenarios.[6]

Wargaming in a Nutshell

Wargaming is a form of serious gaming in which gameplay is blended with real-world strategy. While not exhaustive, wargames take various forms, including board games, scaled miniatures, tabletop exercises, and computer-based simulations. They can be commercially available or custom-built, even with simple materials, as demonstrated in the Wrens' case. Hybrid versions that blend physical and digital elements have also gained popularity. Crucially, wargames do not involve the actual deployment of military forces. Such activities fall under field exercises instead.[7]

Depending on their design, wargames are open or closed, featuring turn-based strategies or real-time decision-making.[8,9] Moreover, many wargames incorporate detailed maps and role-playing elements to enhance immersion. However, the level of realism varies depending on the game's intended focus on strategic depth, historical accuracy, or creative exploration.

While wargames can be recreational, they are widely applied in professional settings for policy analysis, education, and team building. From the Prussian 'Kriegsspiel' to modern defence simulations, wargaming has evolved into an important tool for military strategy, business simulations, and crisis management.

In a structured, safe-to-fail environment, free from real-world consequences, wargaming allows participants to engage with scenarios of conflict or competition by presenting their decisions that dynamically influence one another.[10] Embedded in a culture that allows questions and mistakes, this interplay supports brainstorming, knowledge building, and strategic refinement, helping organizations explore alternative courses of action (COAs) and prepare for unforeseen contingencies.[11]

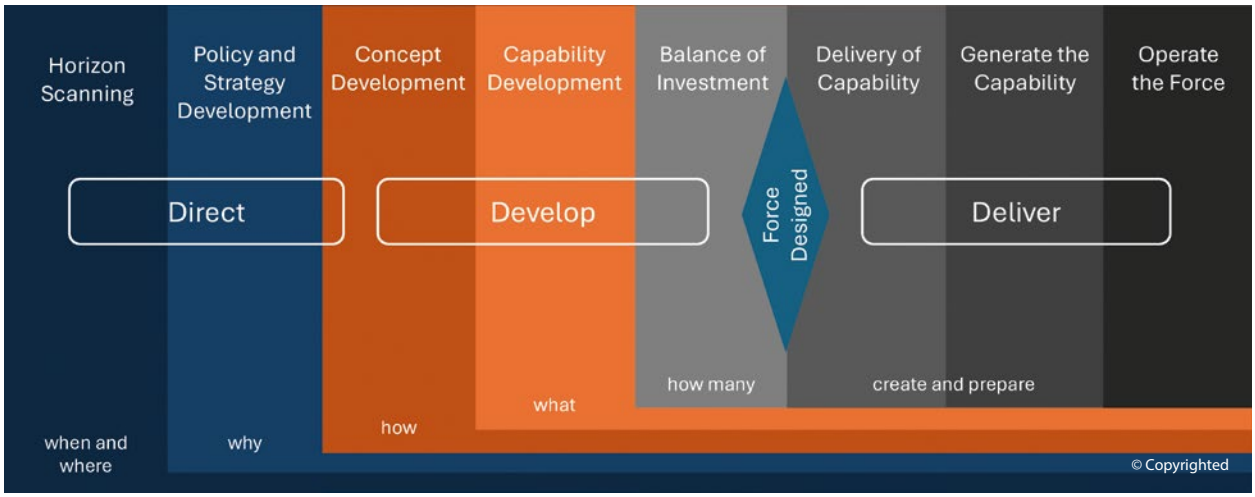


Figure 1: *Force Development Model*
(adapted from UK Defence Experimentation for Force Development Handbook V2 [2021]).[12]

Control and adjudication serve as the foundation of any wargame. Participants can determine outcomes, which fosters engagement. Outcomes can also be overseen by a facilitator or adjudication team to ensure structure and impartiality. Its rules may be fixed, prescribing unit movement and engagement, or flexible, relying on logic and best practices.

Wargaming's Role in Future Force Design

Future force design – or force development – aims to anticipate future force requirements by analysing potential adversaries' intents and strategies and informing defence planning. It includes a strong transformational element, as it shapes (and reshapes) military capabilities to meet evolving operational demands. It enables NATO and nations to proactively adapt their future capabilities to emerging threats.

As illustrated in Figure 1, force development follows three key phases: Direct, Develop, and Deliver. Wargaming plays a crucial role in the development phase, particularly in Concept and Capability Development, the steps that translate strategic foresight and horizon-scanning insights into impactful future capabilities. Wargaming is a valuable tool in these stages as, through the active engagement with dynamic and unpredictable situations, it enhances the participants' critical thinking and adaptive capacities, which results in better performance in decision-making, performance evaluations, and resource allocations.

The first step, Concept Development, typically involves abstract, high-level assessments, as this formative stage centres on exploring foundational ideas and broad strategic frameworks. As concepts evolve and gain structure, wargaming often becomes a more focused and applied exercise during Capability Development, supporting the evaluation of more concrete and practical applications.

Strengths and Limitations of Wargaming

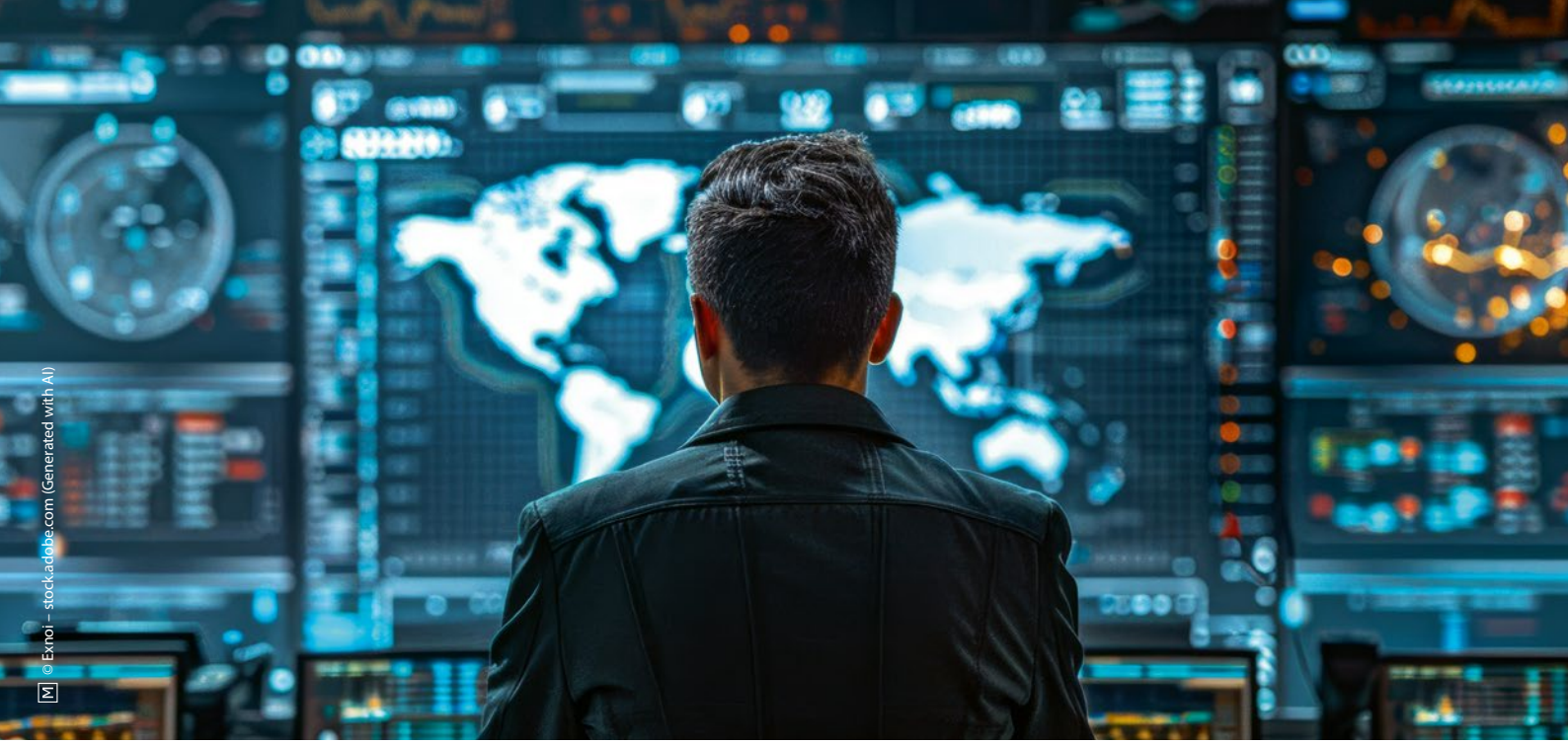
Wargaming's interactive and immersive nature enables the identification of hidden vulnerabilities and the exposure to flawed assumptions.[13] It especially facilitates a deeper understanding of complex systems.

While predicting the future may never be possible, wargaming can provide valuable foresight.

Wargaming intrinsically places the interaction with and between human participants at its core. This interactive element sets wargaming apart from related methodologies, such as modelling and simulation, which prioritize computational processes. While wargaming incorporates elements of simulation, by anchoring its practice in human involvement, wargaming encourages dynamic decision-making and adaptability in ways computational methods cannot replicate.

However, it must be acknowledged that wargaming brings a qualitative perspective – with limited validation power – rather than science to the table. Wargames can illustrate that something is plausible, narrowing down the number of probable outcomes, but they will not be able to predict outcomes with certainty.[14]

Designing wargames that accurately forecast outcomes remains 'the Holy Grail' of wargame designers.[15] They rely on constructed scenarios that, at best, offer general truths rather than precise predictions. Conway's Law provides further caution, suggesting that biases, silos, and structural limitations of wargame creators may unintentionally shape a game's scope and limit its broader integration.[16]



Wargames can introduce complex global dynamics and interconnections, allowing decision-makers to understand and anticipate future challenges.

Another scoping challenge lies in participant expertise. On the one hand, participants must be qualified and well-informed within their designated areas of expertise in the wargame. An evaluation of autonomous collaborative platforms (ACPs), for instance, may seek participants with backgrounds in air or drone operations. However, relying exclusively on experts from highly specialized, yet directly related, disciplines can be limiting. While their insights are valuable, they may lack the interdisciplinary perspectives needed to translate findings effectively into multi-domain contexts or to account for logistical, industrial, and other kinds of constraints further down the chain.

'Recent advancements in the air and space domains reflect wargaming's growing role in formulating and evaluating concepts for future force design.'

Wargaming further holds the risk of false lessons being identified from a single run of a wargame.[17] However, the considerable time required for setup, execution, and analysis, even when supported by computer aids, often limits the practicality of conducting multiple iterations to refine or validate outcomes. What adds to this is that the human-centred nature of wargaming restricts its ability to replicate scenarios with precision, thereby constraining the depth and breadth of insights that could be gained through repeated iterations. No two wargames will ever be alike.[18]

Despite these limitations, wargaming remains a powerful tool for stress-testing ideas, uncovering potential risks, and fostering innovation. It does not provide absolute certainty but offers a structured environment for exploring possibilities, allowing decision-makers to anticipate challenges and refine strategies in ways other methodologies cannot.

Key Considerations for Wargaming Within Force Design

Formulating operational concepts within future force design demands a nuanced grasp of interdependencies and interactions rather than focusing solely on tactical mechanics. As argued here, wargames offer a powerful tool for qualitatively analysing and navigating these complexities. In this sense, wargames can also serve as a warm-up exercise, fostering the right mindset among participants and preparing them to approach force design challenges with a deeper, more interconnected perspective.

The Wrens' wargame demonstrates that generating valuable insights does not always require complex simulations. Even though wargames will always need a certain amount of commitment from developers, planners, and participants, their simple yet effective exercise demonstrates how structured discussions, even in minimal settings, can educate and refine strategic thinking, enhancing operational effectiveness. Because accessible, resource-efficient approaches require lower time demands and reduce logistical barriers, they are convenient to implement and encourage interdisciplinary engagement and broader participation. This facilitates meaningful dialogue on how various domains shape operational effects in a theatre. Their production speed also allows a quicker response to a sponsor's request.[19] Additionally, their ability to conduct repeated runs is a key advantage, as streamlined formats enable rapid iteration, revealing patterns and insights that might otherwise go unnoticed. In this way, these simpler setups may allow for deeper assessments of complex operational contexts.

However, while simple wargaming formats support iterative learning and broad engagement, specific operational contexts demand more sophisticated analyses – for instance, when aiming for so-called 'deep dives' to understand mission-specific or theatre-level challenges better. In such cases, integrating advanced models, potentially supported by computer-aided tools, can offer a more thorough exploration of operational complexities. AI, for example, could assist in the adjudication process, enable adaptive scenario generation, or contribute to enhanced realism. Carefully selecting diverse participants, both in wargame design and execution, is also important, to minimize blind spots and ensure broader applicability across domains.

Additional methodological refinements can improve wargaming's validation potential. For instance, integrating structured scenario design with real-world data strengthens the analytical rigour of wargaming exercises, ensuring their relevance for operational concept development. Another option is to narrow the scenario focus to typical and high-priority events, which enhances realism and applicability, leading to more precise and actionable insights.

Nevertheless, even with these methodological enhancements, wargaming remains a tool for iterative refinement rather than rigid validation. Especially in the conceptual stages of force development, wargaming should not be viewed as a predictive tool but as a powerful method for qualitative assessment and idea refinement. It should be regarded as a mechanism for identifying plausible and implausible approaches, informing strategic adjustments rather than providing definitive conclusions. The insights generated through wargaming generally need further evaluation through complementary analytical methods. Therefore, it should be combined with other methods to achieve comprehensive results.[20]

'The "losing" team frequently derives the greatest lessons from wargaming, as failure tends to drive more refined, resilient, and adaptable solutions.'

As a final point, it is essential to recognize that wargaming, particularly within the context of future force design, is not about achieving victory. Its true value lies in developing strategic acumen and deepening the understanding of how future forces can effectively navigate operational friction. Paradoxically, the most valuable insights often emerge from setbacks. In fact, the 'losing' team frequently derives the greatest lessons, as failure tends to drive more refined, resilient, and adaptable force structure solutions. Also, wargaming helps to identify failure points early, enabling proactive adjustments to strengthen force design.

How to get started… …just start!

Supporting Entities

- HQ SACT Wargaming and Experimentation Branch (part of HQ SACT Concept and Development Branch (CNDV)).
- Centres of Excellence (CoE); submit a Request for Support (RfS) to assist in the wargaming process.

Wargaming Handbooks

- NATO's Wargaming Handbook (combine with NATO's CD&E Handbook).

Additional guidance can be found in various nations' handbooks (available in English):

- Defence Wargaming Handbook (UK)
- Bundeswehr Wargaming Handbook (Germany)
- CICDE Wargaming Handbook (France)

Examples and Initiatives

- Audacious Wargaming is one of the lines of delivery led by HQ SACT in its effort to better understand the challenges facing the Alliance's Military Instrument of Power.
- PS-177 NATO Wargaming Practitioner Course at NATO School Oberammergau.
- Wargaming Initiative for NATO (WIN), co-organized by Germany, France, and Italy; WIN 24 marked the 200-year anniversary of the Prussian Kriegsspiel.
- NATO STO and HQ SACT 2023 Alliance Space Deterrence Framework Wargame, including a two-year series of wargames seeking to increase the 'Space Intelligence Quotient' of NATO Permanent Representatives.

Off-The-Shelf Popular Games

- Operational Wargame System (Military off the Shelf)
- Littoral Commander (Commercial off the Shelf)

Conclusion

Wargaming remains a vital and powerful instrument for refining operational concepts within force design. While it cannot predict the future, its hallmark – its emphasis on the human element – ensures it uniquely fosters operational art into the equation. Though its limitations must be acknowledged, wargaming narrows the spectrum of probable outcomes and improves decision-making by refining human judgment and creativity. Although the analytical power of wargaming can be enhanced by leveraging emerging technologies, such efforts can distract from what should be the focus of a wargame: its human-centric nature, i.e., the players' decision-making. By ensuring that wargaming is integrated into a broader analytical toolkit, both NATO and NATO members can maximize wargaming's contribution to shaping resilient and future-proof force structures in their evolving security landscapes.

Afterword

The Royal Netherlands Air and Space Force (RNLASF), in partnership with Royal NLR, TNO, and JAPCC, is accelerating efforts to embed wargaming within a rigorous, comprehensive methodological framework. This collaborative undertaking is geared to systematically shaping actionable and future-looking operational concepts that strengthen a resilient force structure in continued alignment with national and NATO priorities. ●

1. The Western Approaches Tactical Unit (WATU), created in January 1942, recruited Wrens with demonstrated mathematical skills for their wargame scenarios (About Western Approaches. Retrieved from https://liverpoolwarmuseum.co.uk/about/#:~:text=The%20Western%20Approaches%20Tactical%20Unit%20(WATU)%20was,from%20the%20Women%27s%20Royal%20Naval%20Service%20(Wrens); Strong, E. (2017). Wargaming the Atlantic War. Retrieved from https://www.professionalwargaming.co.uk/171210WATU-MORS.pdf).
2. Only some of the Wrens had been to sea and none had ever seen a submarine (Castelow (2023). Wrens, Wargames and the Battle of the Atlantic. Retrieved from https://www.historic-uk.com/HistoryUK/HistoryofBritain/Wrens-Wargames-North-Atlantic/).
3. E.g. NATO Washington Summit Declaration (2024); NATO NWCC (2021); Schroll, T. (2023), Enhancing NATO Air and Space Power in an Age of Global Competition. JAPCC Journal 35; NATO (2025). NATO Space Domain, A New Frontier of Security. Retrieved from https://ac.nato.int/archive/2025-2/nato-space-domain--a-new-frontier-of-security.
4. NATO HQ SACT, for instance, has recently published a NATO Wargaming Handbook, launched the Experimentation and Wargaming Branch, and organises wargaming events such as WIN 24 (Allied Command Transformation (2023). Allied Command Transformation Engages in Audacious Wargaming Activities to Refine the Alliance's Military Instrument of Power. Retrieved from https://www.act.nato.int/article/allied-command-transformation-engages-in-audacious-wargaming-activities-to-refine-the-alliances-military-instrument-of-power/.

5. e.g. NATO (2023). NATO STO hosts wargame on Space Deterrence. Retrieved from https://www.sto.nato.int/SitePages/newsitem.aspx?ID=3898#:~:text=The%20NATO%20Science%20and%20Technology,%2Dsur%2DSeine%2C%20France; Anderson K. (2025). The Missing Pieces of NATO's Autonomous Collaborative Platform Strategy. JAPCC Journal 39.
6. Perla, P. P., & Mc Grady, E. (2011). Why Wargaming Works. Naval War College Review.; Mouat, T. (2022). The use and misuse of wargames. Scandinavian Journal of Military Studies; NATO STO (2024). Decision-Making for the Future. STO-EN-SAS-195 Report.
7. Perla, P. P. (1990). The art of wargaming: A guide for professionals and hobbyists. US Naval Institute.
8. In open wargames, players can see each other's actions, units, and positions. In closed wargames, they play 'blind', simulating the fog of war. Closed wargames emphasize reconnaissance and intelligence-gathering in scenarios where information is not fully available (decision-making under uncertainty). (Perla, P. P. (1985), An Introduction to Wargaming and its Uses. Centre for Naval Analyses; Brunel University London (2015). Connections UK. Retrieved from https://www.professionalwargaming.co.uk/24TypesOfWargames.pdf.
9. In turn-based strategy games, players take turns with a designated amount of time to plan and execute their actions. This allows for careful planning and strategic thinking without the pressure of real-time events. In real-time strategy games players make decisions and execute their moves 'on the fly', which requires and trains the ability to adapt to rapidly changing situations. (Retrieved from https://programcritique.com/real-time-vs-turn-based-comparing-the-two-types-of-strategy-games/; Dockhorn, A. et al. (2020), STRATEGA – A General Strategy Games Framework. CEUR Workshop Proceedings. Retrieved from https://ceur-ws.org/Vol-2862/paper30.pdf).
10. Bundeswehr (2024). Wargaming Handbook.
11. Perla, P. P., & Mc Grady, E. (2011). Why Wargaming Works. Naval War College Review.; Mouat, T. (2022). The use and misuse of wargames. Scandinavian Journal of Military Studies; NATO STO (2024). Decision-Making for the Future. STO-EN-SAS-195 Report.
12. NATO is currently working on a similar, but NATO-specific version of a Force Development Model.
13. Downes-Martin, S. et al (2017). Validity and Utility of Wargaming. Working Group (Vol. 2).
14. UK MoD (2020). Defence Wargaming Handbook.
15. Mason, R. (2023). Prediction and Validation in Wargaming: Are they possible? Retrieved from https://www.lecmgt.com/blog/prediction-and-validation-in-wargaming-are-they-possible/.
16. Conway's Law: '[O]rganizations . . . are constrained to produce designs which are copies of the communication structures of these organizations.' (Conway, M. (1968). How do Committees Invent. Datamation 14 (Vol. 4), pp. 28–31).
17. UK MoD (2020). Defence Wargaming Handbook.
18. Allied Command Transformation (2023). NATO Wargaming Handbook.
19. CICDE (2024). Wargaming Handbook (English version).
20. Allied Command Transformation (2023). NATO Wargaming Handbook.

ABOUT THE AUTHORS

Mr Antoine de Reus

MSc, Royal NLR – Netherlands Aerospace Centre

Antoine de Reus leads the Future Force Design team at Royal NLR, developing future-proof air and space power capabilities in a strategic collaboration with RNLAF. His team strengthens NLR's operational and strategic expertise while advancing methodologies for force design. With a foundation in electrical engineering, Antoine has worked across diverse domains, including human-machine interfacing & teaming and advanced display systems such as head-up and helmet-mounted displays for both rotary and fixed-wing applications. In 2012, he completed the Advanced Airpower Course at the Netherlands Defence Academy, reinforcing his expertise in airpower foundations. Since 2022, Antoine has also served as programme lead for information-driven operations, one of NLR's key strategic initiatives.

Lieutenant Colonel Gwendolyn Bakx

PhD, NLD Air and Space Force, JAPCC

Lieutenant Colonel Gwendolyn Bakx works on topics regarding air leadership and transformation in JAPCC's C5ISR+Space branch. She has flown the Alouette-III, BO-105, and CH-47 and deployed to missions in Bosnia, Kosovo, Iraq, and Afghanistan. Her academic credentials include two master's degrees (labour psychology and human factors & system safety) and a PhD in safety within Large-Scale Socio-Technological Military Systems. She has served as deputy commander of the Aircrew Survival School, as flight safety officer at RNLAF HQ, and held multiple positions at the Netherlands Defence Academy, among which as Associate Professor in Human Factors and System Safety. Gwendolyn contributed to the Future Operating Concepts for Air and Space at RNLAF's Air and Space Warfare Centre.

LEADING THE WAY IN OPEN MISSION SYSTEMS

snc®

sncorp.com

Redesigning NATO's Targeting Enterprise for Peer Conflict

Digitizing the Kill Chain at the Tactical Edge

By Air Vice-Marshal Mike Hart (ret.)

Introduction and Key Arguments

NATO's targeting enterprise is not fit for purpose. As a legacy of two decades of counterinsurgency (COIN), counterterrorism (CT), and wars against weak nation states, the Alliance lacks the targeting capability required to meet the challenges of a potential war with a peer adversary. It is incapable of handling volumes of data at pace and lacks the capacity to prosecute hundreds of targets per day. It requires a full redesign.

An approach focused on incremental modernization (e.g. by the incorporation of tactical data links) will not suffice. Full digitization, based on cloud computing, dynamic artificial intelligence (AI), and empowering warfighters on 'the Edge' to convert data into targets can provide a robust and versatile platform, increasing capacity more than ten-fold without requiring more human targeteers.

Technology is only part of the answer. To produce a targeting system fit for modern war requires a mindset shift that sees the targeting enterprise as a weapon system, critical to deterrence via enhanced lethality. There are major issues of doctrine and policy that must be addressed, including the relationship of the human to AI in tactical targeting, the balance between centralised and decentralised targeting, the delegation of authorities to expedite kill chains, and the training of a generation of commanders (at all levels), lawyers, and politicians so that they are comfortable with limited, and sometimes no, direct human involvement in the application of lethal force. Putting the right policy framework in place will enable very high-tempo and highly automated decentralised operations at tactical echelons within acceptable risk tolerances, whilst retaining centralised control of strategic targeting where and when appropriate.

There is an urgency to this: redesigning the targeting enterprise is necessary before the exigencies of war reveal the inadequacies of the current system, prevent NATO from exploiting its technological advantage, and in extremis, result in strategic failure.[1]

NATO's current targeting enterprise is outdated and unfit for high-tempo conflict against peer adversaries, lacking the speed, scale, and automation required to process and engage hundreds of targets daily.

NATO's Targeting Enterprise: Fit for War?

The genesis of this article was a question from a NATO officer I worked with during Operation Unified Protector (Libya) in 2011. Frustrated by the operation's obsolete technology and 'Post-it note' targeting methods, he proposed that NATO targeting should operate via Tactical Data Link (TDL). TDL would undoubtedly improve the process, but the hard truth is that more is required; indeed, the complexity, tempo and capacity demanded by a major conflict require nothing less than a fully redesigned digitised targeting enterprise, capable of operating at pace, generating and engaging targets from strategic to tactical, from Core to Edge.

In Iraq and Afghanistan, the US and its allies relied on layered and massed intelligence, surveillance, and reconnaissance (ISR) to feed centralised processing, analysis, and distribution facilities, which then produced fused intelligence. Whilst this process could be expeditious, especially for troops in contact, it depended on moving large data volumes from (primarily) airborne sensors, often to different continents for analysis, before intelligence products returned to the operational theatre. This operational model relied on several key assumptions: command of the air (allowing vulnerable ISR aircraft to operate), uncontested access to space, and freedom from effective cyber disruption. Furthermore, facing technologically unsophisticated opponents meant Command and Control (C2) itself was largely invulnerable to kinetic or cyber-attacks. In a future conflict where NATO is unable to easily overmatch its opponent, none of these assumptions will hold true.

In a future major conflict, air, land, maritime, space, cyber, and electromagnetic domains will be intensely contested, with advantage ebbing and flowing across domains and time. Disruption to C2 is inevitable. Units or groups of units may choose to disconnect from the C2 system. Equally they may be forcibly disconnected, either by the physical destruction of headquarters or communications systems and attacks across the electromagnetic spectrum.

To prevail, NATO forces will need to be able to deploy full capabilities toward the front lines, operating in a way that allows cross-domain and multinational operations even when hierarchical C2 is effectively lost.

So long as the ability to securely collect, move, process and exploit data exists on the front lines, technology can enable this, but political and military culture is also critical. Fighting fast in a highly contested environment requires initiative and confidence based on a clear understanding of tactical, operational and strategic intent and the ability to maintain real time understanding of a rapidly changing battlespace. In such an environment a culture of Mission Command with authorities delegated to the lowest appropriate tactical effector could be the difference between success and failure.

NATO's targeting enterprise is currently designed, configured, and resourced to develop and prosecute only a small number of targets per day, typically as single strikes. This limited capacity was starkly evident during Operation Unified Protector in Libya (2011); even against a relatively weak state, NATO struggled to service just 20–30 targets daily, a difficulty stemming significantly from inherent enterprise constraints, not solely from limited aircraft availability. Such performance will be completely inadequate in a high-tempo war against a peer adversary, which will demand the engagement of hundreds of targets daily across all echelons. Key constraints exacerbating this challenge include the limited pool of targeteers (who require mandatory formal training and accreditation), current systems' inability to manage data at the pace required for coherent targeting, and the legal and policy friction inherent in a multinational alliance.

Unlike in COIN and CT, warfare against a state adversary requires an understanding of the enemy as a system of related systems. This perspective will enable NATO to disrupt, degrade, and coerce the adversary through the systematic and sustained application of kinetic and non-kinetic force. Such an approach, in turn, implies equally systematic pre-preparation. Contemporary conflict also demands a targeting system that can seamlessly pivot between deliberate targeting (e.g., pre-planned actions like countering IADS) and dynamic targeting (e.g., immediate responses like suppressing enemy artillery).

Given the volume of potential targets, the overwhelming volume of data available and required, and the need to analyse data at pace, matching targeteers to requirements is not practical without a radical shift in the human/technology balance. To fight effectively, full digitization of NATO's targeting enterprise is essential; its primary intent should be a more than tenfold increase in capacity without expanding the human workforce.

Design Principles

Targeting should be viewed not merely as a process but as a weapons system, whose demonstrable lethality is critical for enhancing deterrence. Effective digitization, therefore, must serve as a demonstrable and significant multiplier of this lethality. Consequently, a digital targeting system itself becomes a key pillar of deterrence, vital for ensuring traditional deterrents are collectively more potent than the sum of their parts.

A digitised NATO targeting enterprise requires the following:

- Survivable ISR from collect to processing, exploitation, and dissemination (PED).
- Strategic to tactical targeting – from critical infrastructure deep inside an adversary state to a single artillery piece on a battlefield.
- Deliberate and dynamic targeting (i.e. both pre-planned and responsive).
- Integrated effects across all domains (e.g. kinetic and non-kinetic such as cyber and electromagnetic warfare).
- Multiple classification inputs from multiple sources.
- Capacity: High data volume and ops tempo enabled by cloud computing and full AI integration.
- Resilience: The ability to function when C2 is disrupted. Capability, capacity, and redundancy from Core to Edge, including the ability for NATO elements to develop and prosecute dynamic targets at the tactical level.
- Tempo: The ability to fight at machine speed. This implies the full use of AI and automation, including automatic data fusion from multiple platforms and sensors across all domains and automated weapon system direction and weapons delivery.

- Interoperability: National (cross-government) particularly to integrate kinetic and non-kinetic action and international (allied). The latter may increase in importance if the US steps back from leading NATO operations as was the case in Libya.
- Adaptability: The ability to quickly integrate new sensors and platforms within a technology stack.

Policy Framework

Targeting is subject to policy and legal controls that, in practice, vary throughout the course and across the spectrum of conflict. In grey zone confrontations, these controls are typically very tight to ensure actions send the correct political signals and minimize the risk of inadvertent escalation. Conversely, during high-tempo, state-versus-state conflict, engagement of some strategic targets will necessarily require tight control to avoid tripping nuclear thresholds. Others, particularly tactical targets such as enemy artillery or missile systems, will require immediate engagement at a speed faster than human decision-making can achieve.

The need for graduated responses drives a dynamic policy approach akin to a 'command rheostat' that determines engagement authorities for different targets and situations. Such adaptations are not controversial; as there are precedents for such control variability as seen in Libya, Iraq, and Syria. What is fundamentally new in a digitised ISR and targeting enterprise is the need to incorporate automation. The system must be configured to support both highly centralised human decision-making, and, when conditions demand, complete autonomy. This includes an AI-based digital system capable of matching weapon to target, providing mensurated coordinates, and directing engagement – potentially without direct human involvement in the decision loop.

This reliance on automation places a premium on the technological assurance of the targeting platform and its diverse data inputs, whether from highly classified traditional ISR, or through rapid, automated analysis and fusion of open-source intelligence, including social media. It will also demand a significant, concerted effort to train the targeteers, lawyers, officials, commanders, and politicians to operate confidently and ethically with systems that involve limited, and in some cases no, direct human control over the application of lethal force.

Display of rocket sections from an intercepted Russian Tochka-U missile in Ukraine.

Technology

A NATO targeting enterprise capable of functioning effectively in a high-tempo conflict, servicing hundreds of targets per day, will demand the capacity to handle vast data volumes at pace. This requires hyperscale cloud computing. For security, this means NATO-operated cloud infrastructure, detached from the public internet, run in Alliance data centres by security-cleared personnel.

The likelihood of electronic and physical disruption, including physical attacks on data centres, C2 nodes, and major intelligence facilities drives an urgent requirement for resilience. Effective combat operations depend on data access; if data resides only on a centralized platform, it becomes extremely vulnerable.

Therefore, the system must be designed with multiple redundancies so that it functions as effectively as possible when attacked. In practice this means enabling units to develop and prosecute targets as close to the tactical Edge as possible. Individual warships, aircraft and land units must be able to continue to collect and use data to target the enemy even when disconnected from NATO or national C2. For instance, in a contested Baltic scenario, diverse multinational assets – such as a Swedish corvette, a Norwegian F-35, and

Finnish land forces – would need to collaboratively share situational awareness and synchronize actions using locally processed data if primary C2 links were severed. This capability requires a distributed cloud architecture, with maximum computing power pushed to tactical levels, enabling disconnected operations for extended periods and re-synchronization with the core when feasible.

Summary

NATO's targeting enterprise is not fit for purpose. It is inadequate to meet the challenges of a large-scale war and is incapable of quickly handling large volumes of data to prosecute hundreds of targets per day. It requires a full redesign.

Technology offers the potential to redesign the NATO targeting enterprise, radically increasing capacity allowing more targets to be prosecuted faster and more accurately. A full redesign, based on cloud computing and dynamic AI, can provide a robust and versatile platform. This approach, which empowers warfighters on 'the Edge' to convert data into targets, could increase capacity more than ten-fold without requiring more human targeteers.

However, technology is only part of the answer. To produce a targeting process fit for modern war requires a mindset shift that sees the targeting enterprise as a weapon system, critical to deterrence via enhancing lethality. With the right policy framework this will enable very high tempo and highly automated decentralised operations at the Edge, within acceptable risk tolerances, whilst retaining centralised control of strategic targeting where and when appropriate.

Addressing these inadequacies is urgent. Failure to act before conflict exposes these flaws would prevent NATO from exploiting its technological edge and could, in extremis, result in strategic failure. ●

1. See Fabian Hoffman: Foreign Policy, 19 May 2025, A Russia – NATO War would look nothing like Ukraine.

ABOUT THE AUTHOR

Mike Hart

By Air Vice-Marshal Mike Hart (ret.)

Air Vice-Marshal (ret.) Mike Hart is Senior Adviser on Defence and Intelligence for Oracle. He spent more than 30 years as an intelligence officer in the Royal Air Force, retiring in 2022. His operational experience encompasses the Middle East, Russia, Africa, the Balkans, and Northern Ireland. Latterly, he worked in key senior appointments in UK Defence Intelligence Operations and ran the UK's cross-government Joint Terrorism Analysis Centre. He worked extensively with allies and is deeply experienced in ISR and targeting. He has wide experience of UK and Allied Intelligence Communities, including Five-Eyes and NATO. Educated at Oxford and Cambridge Universities, he is a Senior Associate Fellow at RUSI and provides geopolitical advice to various think tanks, NGOs and academic bodies.

2025 SC/SRC Meetings with Sponsoring Nations

Aligning Resources and Priorities Through Strategic Discussions

The 2025 Joint Air Power Competence Centre (JAPCC) Steering Committee (SC) and Senior Resource Committee (SRC) meetings were held in Kalkar, Germany, from 11 to 12 June 2025. These meetings play a vital role in keeping Sponsoring Nations informed about JAPCC's Programme of Work (POW) progress and ensuring resources are aligned with the Centre's priorities.

Chaired by Colonel Vito Cracas, Assistant Director of the JAPCC, the SC meeting highlighted JAPCC's continued impact as a catalyst for NATO's improvement and transformation. 'The committee engaged in constructive discussions regarding JAPCC's future direction, as it continues to enhance NATO's air and space capability.' Key topics included manning requirements, the NATO TIER 4 Plan, the Annual Report, Areas of Interest and Focus, internships from Academia, outreach efforts, and JAPCC's role in major events such as the annual JAPCC Conference and COE Cluster Meetings. These discussions underscore the Steering Committee's essential role in shaping JAPCC's trajectory to meet evolving NATO challenges.

Meanwhile, the SRC meeting, led by Colonel Hans-Jürgen Knittlmeier, Host Nation SRC representative, reviewed and closed all action items for 2025. Despite significant staffing shortages, both the SC and the SRC confirmed the JAPCC's growing relevance and influence, evidenced by increased engagement with its publications – such as the JAPCC Journal and White Papers – the high-profile attendance at the annual conference, and a rising number of Requests for Support from member nations. These factors reflect the strong confidence NATO places in the JAPCC's expertise and support.

'...the SC meeting highlighted JAPCC's continued impact as a catalyst for NATO's improvement and transformation.'

The committee also addressed important resource topics including manning, the upcoming budget request for FY 2026, the Medium-Term Financial Plan (2027–2031), a NLD position exchange, and amendments to financial administrative procedures. This comprehensive review ensures that JAPCC remains well-equipped and agile in fulfilling its mission.

Together, the 2025 SC and SRC meetings reaffirmed JAPCC's unwavering commitment to delivering innovative solutions that enhance NATO's air and space capabilities and strengthen collective defence in a dynamic strategic environment. ●

The JAPCC Think Tank Forum

Adapting to the Evolving Modern Warfare Landscape

From 15 to 16 April 2025, the JAPCC and Headquarters Allied Air Command (AIRCOM) jointly hosted the 12th Joint Air and Space Power Think Tank Forum (TTF) at Ramstein Air Base. This year's event was the largest yet, bringing together 31 key NATO and partner organizations from air forces, defence ministries, universities, and research centres. Held in conjunction with AIRCOM's Air Warfare Development Team (AWDT), the forum focused on evolving the Alliance's air and space capabilities to meet the demands of modern warfare.

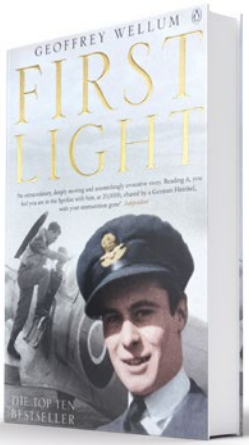
'This year's event was the largest yet, bringing together 31 key NATO and partner organizations…'

Led by AIRCOM Deputy Commander Air Marshal Johnny Stringer and JAPCC Assistant Director Colonel Vito Cracas, the two-day event featured plenary sessions and syndicate discussions on pressing topics such as challenges in air command and control, mission planning, synthetic training, and the integration of cyber and space operations. The forum also explored concepts for autonomous collaborative platforms.

The diverse group of participants shared expertise and insights, fostering robust discussions aimed at identifying gaps and proposing innovative solutions to enhance NATO's operational readiness. The event underscored the importance of collaboration across NATO entities to adapt to the rapidly transforming character of conflict.

Outcomes from the syndicates were consolidated into fact sheets, made available on the JAPCC's secure network (NSWAN JAPCC webpage), and will directly inform ongoing and future Alliance projects, concepts, and training activities.

The JAPCC and HQ AIRCOM extend their gratitude to all participants for their valuable contributions and look forward to continued cooperation in strengthening NATO's air and space power capabilities. ●



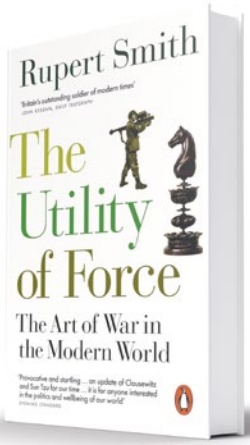
First Light

First Light is a rare kind of war memoir–raw, deeply personal, and emotionally resonant. Geoffrey Wellum, who joined the RAF at 17 and became one of the youngest Spitfire pilots during the Battle of Britain, recounts his journey not as a hero, but as a young man thrust into history. His writing is honest, self-deprecating, and refreshingly unpolished, capturing the thrill of flight, the terror of combat, and the toll war takes on a person's psyche.

What makes this book a must-read is its authenticity. Wellum doesn't just place you in the cockpit–he takes you inside the mind of a boy rapidly hardened by war. His reflections on fear, camaraderie, and identity give the memoir emotional depth beyond typical aviation accounts.

This isn't just for military historians or aviation buffs. It's for anyone interested in how extraordinary pressure shapes ordinary people. At its heart, *First Light* is about growing up fast, surviving what many did not, and reckoning with what comes after. If you're looking for a wartime memoir that balances excitement with humanity, this one earns its place on your shelf. ●

By Geoffrey Wellum; Penguin Books, 2003
Reviewed by Major Tamás Oszlár, HUN AF, JAPCC



The Utility of Force: The Art of War in the Modern World

In *The Utility of Force*, General Rupert Smith, a seasoned British commander, dismantles traditional notions of warfare with unsettling precision. His central thesis is deceptively simple: the wars we fight today–'wars amongst the people'–are no longer about decisive battlefield victories between nation-states, but about influence, legitimacy, and political resolution in complex, decentralized environments. Drawing on historical insights from Napoleon to the Balkans, Smith demonstrates that military power is increasingly ill-suited to deliver strategic outcomes unless paired with coherent political objectives.

What makes this book essential is not only its clarity in explaining Clausewitzian theory, but its sharp critique of Western post-Cold War military doctrine. Smith's personal experience in Bosnia lends authenticity to his call for integrated operations–where military force, diplomacy, and development agencies work in concert. He is strongest when diagnosing the problem, though his prescriptive solutions are dense and occasionally nebulous.

So what? In an age defined by hybrid threats, insurgencies, and prolonged interventions, *The Utility of Force* offers a sobering lens for military professionals, policymakers, and informed citizens alike. Its enduring value lies in forcing readers to confront a hard truth: overwhelming force alone does not bring peace. This is not a quick read–but it is a necessary one. ●

By Rupert Smith; Penguin Books, 2019
Reviewed by Major Luke Stensberg, US SF, JAPCC

STATE OF THE ART MARKSMAN

The Skyranger 30 and Skyranger 35 from Rheinmetall Air Defence in Zurich are the mobile all-in-one solutions against current and future airborne threats.

Move

The Skyranger turret on any proven and highly mobile armoured vehicle, guarantees protection in all situations, whether it is on or off roads.

Sense

The Skyranger commander monitors the airspace autonomously with its own sensor suite and/or via a higher echelon sensor network. The Skyranger reliably detects, classifies and acquires even small flying objects while on the move or in stationary deployment.

Defend

The revolver guns in their respective calibre (30 or 35 mm), combined with the airburst ammunition deliver impressive performance optimised to engage airborne threats such as drones and cruise missiles with unmatched precision. Customer-specific guided missiles in the Skyranger 30 variation additionally extend the spectrum of engagements and range.

www.rheinmetall.com

LOCKHEED MARTIN

INTEGRATED AIR POWER: STRENGTHENING ALLIED DEFENSE AND CONNECTING THE BATTLESPACE WITH UNMATCHED CAPABILITIES

Learn More