NATO SECURITY FORCE ASSISTANCE CENTRE OF EXCELLENCE

Security Force Assistance Approach in Multi-Domain Operations



NATO SFA COE RESEARCH PAPER

2026

Security Force Assistance Approach in Multi-Domain Operations

Enabling NATO's Multi-Domain Advantage through Partner Forces



NATO SECURITY FORCE ASSISTANCE CENTRE OF EXCELLENCE

This page is intentionally left blank

Security Force Assistance SFA approach in Multi-Domain Operations

Enabling NATO's Multi-Domain Advantage through Partner Forces

NATO SFA COE, Rome, 2026

© 2026 by NATO Security Force Assistance Centre of Excellence.

All rights reserved.

This is a product of the NATO Security Force Assistance COE. It does not represent the NATO opinions or policy, and it is designed to provide an independent position. No part of this publication may be reprinted, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the NATO Security Force Assistance Centre of Excellence. This restriction does not apply for making digital or hard copies of this publication for internal use within NATO or for personal or educational use when for non-profit or non-commercial purposes, providing that copies bear a full citation.

NATO SFA COE Publications
Via della Stazione di Cesano 423, 00123, Rome, Italy
Phone: +39 06 469163511
E-mail: natosfacoe@nsfacoe.org
Web: www.nsfacoe.org

LEGAL NOTICE

This publication contains the opinions of the respective authors only. They do not necessarily reflect the policy or the opinion of NATO SFA COE, NATO or any Agency or any Government and International Organizations. NATO SFA COE may not be held responsible for any loss or harm arising from the use of the information contained in this publication and is not responsible for the content of external sources, including external websites referenced in this publication.

ISBN 9788894641561

About NATO Security Force Assistance Centre of Excellence

When the Alliance speaks today of acting across land, maritime, air, space, and cyberspace as a single orchestrated whole, it is describing far more than a new operational concept. Multi-Domain Operations (MDO) mark a change in the very grammar of military effectiveness. Advantage no longer resides within any one domain; it is generated by the speed and coherence with which activities are orchestrated across all of them — and, increasingly, across the boundary that separates military action from the political, civil, economic, social, information, and infrastructure elements of shared operating environments.

It is precisely at that boundary that Security Force Assistance (SFA) does its work. For all the sophistication of MDO, NATO rarely operates alone. Its effectiveness in shaping, contesting, and fighting is amplified by partner nations whose forces and institutions absorb, sustain, and contribute to MDO. This is the conviction that animates the present research paper: that SFA is not a supplementary activity at the margins of MDO, but a structural enabler of it. Where partner forces are resilient and interoperable, the Alliance's multi-domain advantage extends; where they are not, it is constrained at its most critical interface — with the partner nation itself. This is the perspective that the NATO Security Force Assistance Centre of Excellence was established to advance. As an accredited International Military Organisation, sponsored by Italy, Albania, and Slovenia, with Austria as a Contributing Participant, the Centre supports the Alliance across all four pillars of NATO's transformation — concept development and experimentation, doctrine and standardisation, education and training,

and analysis and lessons learned. We pursue that mission through a holistic, multidisciplinary approach, keeping the security and well-being of populations at the centre of our thinking, and drawing on a network of partner Centres of Excellence, international organisations, academia, and industry whose collective expertise is today our most valuable contribution to NATO and its member nations.

This study reflects that network in its very composition. It brings together the contributions of fellow Centres of Excellence across the domains, the operational insight of NATO Mission Iraq, and the perspective of civilian stakeholders, in order to examine how SFA must adapt — in doctrine, in resourcing, and in the metrics by which we measure success — if it is to remain effective in a multi-domain environment. The questions it raises are demanding ones, and the paper does not shy away from the gaps and limitations that remain. That, too, is the Centre's purpose: to sustain NATO's transformation by promoting the cycle of learning, changing, and adapting on which the Alliance's enduring advantage depends.

I commend this work to military and civilian readers alike, in the hope that it will inform the deliberate, patient effort of building partners capable of acting with us across every domain.

"We are made for cooperation, like feet, like hands, like eyelids, like the rows of the upper and lower teeth. To act against one another, then, is contrary to nature."

-Marcus Aurelius, *Meditations*

Col. Massimo Moncada

Director,
NATO Security Force Assistance Centre of Excellence

Foreword

It is with great pleasure that this foreword introduces *Security Force Assistance Approach in Multi-Domain Operations*, a timely and important contribution to NATO's ongoing adaptation for an increasingly complex strategic environment. As the Alliance advances its understanding of Multi-Domain Operations, this research paper makes a clear and compelling case that Security Force Assistance is not a supporting activity at the periphery of Alliance action, but an essential enabler of NATO's operational effectiveness through and with Partners.

NATO's strategic advantage increasingly depends on the speed, coherence, and resilience with which effects are generated across land, maritime, air, space, and cyberspace. Yet the Alliance does not act in isolation. Across crises, deterrence activities, and operations, NATO works alongside Partners whose capacity, institutional resilience, and interoperability have a direct bearing on mission success. In that context, Security Force Assistance must be understood not simply as a capacity-building function, but as a key instrument for enabling Partners to contribute meaningfully within a multi-domain operating environment.

This paper is especially valuable because it recognizes that Multi-Domain Operations are not achieved by integrating military effects alone. They also require the integration of planning, decision-making, information flows, institutional capacity, and supporting civil functions across a broad

spectrum of actors and domains. For SFA practitioners, this means moving beyond narrowly scoped, domain-specific assistance models and toward approaches that build Partners able to absorb, sustain, coordinate, and employ capabilities in ways that are operationally coherent with Alliance objectives. In practical terms, the paper underscores that resilience, interoperability, education, governance, and cross-domain awareness are no longer complementary considerations; they are central requirements for effective SFA in the multi-domain era.

A major strength of this research lies in the breadth of expertise brought to bear. Under the leadership of the NATO Security Force Assistance Centre of Excellence, this work draws on contributions from seven Centres of Excellence, alongside operational insight from NATO Mission Iraq and perspectives from civilian stakeholders. That collaborative approach is significant. It reflects the very logic of Multi-Domain Operations: no single domain, function, or institution can fully comprehend or address the complexity of the contemporary operating environment alone. By assembling expertise from across the NATO enterprise, this publication demonstrates how the Alliance's innovation ecosystem can produce practical, integrated thinking for real-world applications.

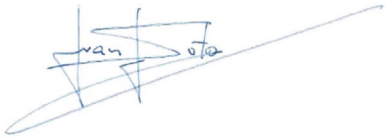
The paper also provides an important conceptual shift for the SFA community. It challenges planners and practitioners to think less in terms of isolated capability development and more in terms of enabling effects across interconnected systems. This is particularly important when working with Partners whose force structures, institutional maturity,

technological baselines, and operational constraints differ considerably from those of NATO Allies. Building Partners capacity for a multi-domain environment therefore requires more than the transfer of tools, platforms, or procedures; it requires sustained efforts to strengthen institutions, improve coordination, reinforce enabling architectures, and support decision advantage under conditions of uncertainty and contestation.

For Allied Command Transformation, the implications are clear. Transformation is not only about developing new concepts or integrating advanced capabilities within NATO forces; it is also about ensuring that the Alliance's Partnerships evolve in step with the changing character of warfare. If NATO seeks to preserve strategic relevance and operational credibility in future crises and conflicts, then it must invest in SFA approaches that are adaptive, coherent, and aligned with the demands of Multi-Domain Operations. This research paper helps illuminate that path.

This foreword therefore commends the authors and contributors for producing a work of both conceptual depth and practical relevance. Its insights will be of value to military leaders, planners, educators, and civilian stakeholders engaged in capability development, Partners engagement, and operational design across the Alliance. More importantly, it should serve as a catalyst for continued thinking on how NATO can strengthen its ability to operate with, through, and alongside Partners in an era defined by interconnected challenges across all domains.

The Alliance's future advantage will rest not only on the capabilities it fields, but on the strength of the networks, Partnerships, and institutions that allow those capabilities to be integrated and applied effectively. In that regard, this publication makes a meaningful contribution to NATO's transformation agenda and to the continued evolution of Security Force Assistance as a strategic enabler of Alliance action.



Major General Juan José Soto Rodríguez
Deputy Chief of Staff Multi-Domain Force Development
HQ SACT

Contributors

Director

- **Col. Massimo Moncada (ITA-A)**
  Director at the NATO Security Force Assistance Centre of Excellence (NATO SFA COE)

Editor

- **Maj. Filippo Barone (ITA-A)**
  NATO Security Force Assistance Centre of Excellence (NATO SFA COE), Concept Development & Experimentation Branch (CD&E), Experimentation Section Chief

Contributors

- **Lt. Col Gianfranco Pino (ITA-Carabinieri)**
  NATO Climate Change and Security Centre of Excellence (CCASCOE), Concept Development & Experimentation Branch (SCD&E), Head of Standardization

- **Dr. Emil Havstrup**
  NATO Climate Change and Security Centre of Excellence (CCASCOE), Concept Development & Experimentation Branch (SCD&E), Concept Development & Experimentation Officer

- **Col. Aurelio Tassi (ITA-A)**
  NATO Mission Iraq (NMI), former Head, Specialized Programmes Coordination Office (SPCO)

- **Capt. Levent Bahadir (TUR-N)**
  NATO Maritime Security Centre of Excellence (NATO MARSEC COE), Capt. (OF-5), WMD Staff Officer & Acting Head, Concept and Doctrine Branch, Subject Matter Expert

- **Lt Col. Gwendolyn Bakx (NLD-ASF)**
  Joint Air Power Competence Centre (JAPCC), C5ISR & Space Branch, Staff Officer Air Leadership & Transformation

- **Maj. Andrii Davydiuk (UKR)**
  NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Deputy Branch Head, PIMEE NAS of Ukraine, State Service of Special Communications and Information Protection of Ukraine (SSSCIP) of Ukraine

- **Dr. Bianca de Teffé Erb (ITA/USA)**
  Deloitte Italy, EMEA AI Risk Leader

- **Dr. David Mach (ITA)**
  Deloitte Italy, Data & AI Ethics Consultant

- **Dr. Francesca Bajardi (ITA)**
  NATO Security Force Assistance Centre of Excellence (NATO SFA COE), Researcher and Concept Development and Experimentation Branch (CD&E) former Intern.

- **Lt. Col. Andrea Console (ITA-AF)**
  NATO, Space Centre of Excellence (NATO Space COE), Chief of Staff

- **Lt. Col. Peter Schäfer (DEU-A)**
  NATO Civil-Military Cooperation Centre Of Excellence (CIMIC CCOE), Concepts, Interoperability, Capabilities (CIC), Branch Chief

- **Eleonora De Martin (ITA)**
  NATO Civil-Military Cooperation Centre Of Excellence (CIMIC CCOE), Concepts, Interoperability, Capabilities (CIC), Consultant

- **Col. Massimo Di Pietro (ITA-A)**
  NATO Security Force Assistance Centre of Excellence (NATO SFA COE), former Director

- **Marianna Santucci (ITA)**
  NATO Security Force Assistance Centre of Excellence (NATO SFA COE), IR Master Student, Concept Development and Experimentation Branch (CD&E) Intern

- **Lt. Col. Vinicio Restelli (ITA-A)**
  NATO Allied Command Transformation, Multi Domain Force Development, Experimentation and Wargaming Branch, Staff Officer, Experimentation (SFA SME)

- **HQ SACT MDO IPT team**
  NATO Allied Command Transformation

Chapters Index

About NATO Security Force Assistance Centre of Excellence 7
Foreword 9
Contributors 13

CHAPTER 1 — INTRODUCTION 20

1.1 Preamble 20

1.2 Historical Background 23

1.3 Joint Operations vs Multi-Domain Operations 28

1.4 Concept and Objectives of SFA 32

CHAPTER 2 — CLIMATE CHANGE CONSIDERATIONS 35

Impact of Climate Change on the Operating Environment and the Consequences for SFA *37*

2.1 Introduction 37

2.2 Effects of Climate Change 38

2.3 How Climate Change Impacts the Operational Environment 41

2.4 Adapting Security Forces to Climate Change: Challenges, Multilateral Approaches and Capability Development 44

2.5 Conclusion 47

CHAPTER 3 — LAND DOMAIN 49

NATO Mission in Iraq: A Case Study *51*

3.1 Preamble 51

3.2 Strategic-Political Context 52

3.3 Engaging with NATO Partner Nations and Relevant International Organizations 55

3.4 NATO's Role in Iraq's Defence and Institutional Building **59**

3.5 DCB Activities in the Land Domain **67**

3.6 NMI Advisory Effort **72**

3.7 Conclusions **73**

CHAPTER 4 — MARITIME DOMAIN 75

MDO in the Maritime Security Context ***84***

4.1 Introduction **84**

4.2 Cross-Domain Coherence as a Strategic Imperative **87**

4.3 Hybrid Threats and Freedom of Navigation in MDO **91**

4.4 Doctrinal and Training Dimensions of Maritime MDO **94**

4.5 Operationalizing MDO: MSA, CI Protection, and Interdiction **97**

4.6 Kill Chains, Resilient C2, and Unmanned Integration **100**

4.7 Strategic Conclusions: Embedding MDO in Maritime Security **102**

4.8 Toward a Secure and Resilient Maritime Commons **104**

CHAPTER 5 — AIR DOMAIN 107

Understanding the Air Domain for Effective SFA Delivery in a Multi-Domain Context ***109***

5.1 Introduction **109**

5.2 The Air Domain in Modern Conflict **111**

5.3 An Effects-Based, Domain-Agnostic Approach to SFA in an MDO Environment **118**

5.4 Implications for SFA Delivery in an Air-Enabled MDO Context **121**

5.5 Recommendations **123**

5.6 Conclusion **125**

CHAPTER 6 — CYBER DOMAIN 127

The Importance of Cyber-Focused Security Force Assistance in Strengthening Partner Nations' Cybersecurity Resilience and Defence Capabilities ***129***

6.1 Introduction **129**

6.2 Addressing Cyber Threats, Securing Communication Networks, and Sharing Intelligence **143**

6.3 A Relevant Case Study and Best Practice **151**

CHAPTER 7 — ARTIFICIAL INTELLIGENCE AS A CROSS-DOMAIN ENABLER 158

Global Artificial Intelligence and Cyber Trends ***161***

7.1 Geopolitical and Strategic Shifts **161**

7.2 Technological Acceleration and Future Skills Landscape **166**

7.3 Regulatory Evolution and Guidelines **172**

7.4 Threats, Vulnerabilities, and Mitigations **178**

7.5 Strategic Recommendations **189**

CHAPTER 8 — SPACE DOMAIN 197

Space Domain Considerations ***200***

8.1 Introduction **200**

8.2 NATO's Space Infrastructure **200**

8.3 Emerging Threats and Challenges in the Space Domain **204**

8.4 The Space Domain in MDO **207**

8.5 Partnerships, Capacity Building, and SFA **211**

CHAPTER 9 — NON-MILITARY STAKEHOLDER INTERACTION 224

Synchronisation with Non-Military Activities: Enhancing Security Force Assistance through Civil-Military Cooperation in MDO 227

9.1 Introduction 227

9.2 CIMIC: Some Definitions 229

9.3 CIMIC in MDO: Synchronising with Non-Military Activities 231

9.4 Challenges of Synchronisation Between Military and Non-Military Actors in SFA 232

9.5 Implications for SFA 235

9.6 Bridging the Gap Between CIMIC and SFA 237

9.7 Conclusion 243

CHAPTER 10 — CHALLENGES, LIMITATIONS, AND FUTURE DIRECTIONS FOR SFA IN MDO 248

10.1 Introduction 248

10.2 Cross-cutting Challenges 249

10.3 Limitations of This Research 255

10.4 Future Directions 257

10.5 Conclusion 261

APPENDIX 1 – MDO FORMULA 263

APPENDIX 2 - PROJECT MANAGEMENT FOR SFA DELIVERY IN MDO 272

References 291
List of Abbreviations 309

Chapter 1 — Introduction

Maj. Filippo Barone (ITA-A), Author
NATO Security Force Assistance Centre of Excellence (NATO SFA COE), Concept Development & Experimentation Branch, Experimentation Section Chief

1.1 Preamble

This research paper examines Security Force Assistance (SFA) within the framework of Multi-Domain Operations (MDO), with a particular focus on how SFA adapts when the operational environment extends simultaneously across land, maritime, air, space, and cyber domains, and when military action must be synchronised with non-military stakeholders — from governmental organisations and international bodies to private sector actors — whose capabilities and decisions increasingly shape operational outcomes. The question is not merely doctrinal: as NATO's missions evolve away from large-scale expeditionary operations toward sustained advisory and capacity-building engagements, understanding how SFA can generate strategic effects in a multi-domain context has become operationally urgent.

The land domain has been extensively treated in existing literature and NATO doctrine, including AJP-3.16[1] and AJP-3.2[2]. Given this established foundation, this paper does not attempt a comprehensive treatment of land-based SFA. Instead, Chapter 3 focuses on NATO Mission Iraq (NMI) as a bounded case study — not to represent the full breadth of land-domain

[1] NATO 2025 AJP-3.16, Allied Joint Doctrine for Security Force Assistance, Edition B, Version 1.
[2] NATO 2022 AJP-3.2, Allied Joint Doctrine for Land Operations, Edition B, Version 1.

SFA, but to ground the paper's broader argument in operational evidence. NMI was selected because it represents NATO's most developed non-Article 5 capacity-building mission, and because its operational context — hybrid threats, institutional fragility, climate stress, and a contested information environment — encapsulates the multi-domain challenges that recur, in domain-specific forms, across every chapter of this paper.

Each subsequent chapter examines SFA in a specific domain or cross-cutting dimension: climate change and environmental security (Chapter 2), land operations and the NMI case study (Chapter 3), maritime domain (Chapter 4), air domain (Chapter 5), cyber domain (Chapter 6), artificial intelligence as a cross-domain enabler (Chapter 7), space domain (Chapter 8), and civil-military cooperation and collaboration with non-military stakeholders (Chapter 9).

Each chapter contributes to the paper's central argument, not merely by describing domain-specific SFA activity, but by identifying where current doctrine underspecifies the requirements of multi-domain integration. Taken together, these domain findings converge on three axes along which the SFA enterprise must evolve — doctrine, resourcing, and the metrics by which success is judged — which Chapter 10 addresses in turn, and for which Appendix 2 supplies practical instruments. The final chapter synthesises the challenges, limitations, and future directions that emerge across the analysis.

NATO defines MDO as "the orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of

relevance."[3] This definition is deceptively compact. Its operational implication — that effects must be generated faster than adversaries can respond, across physical and digital domains simultaneously — requires a level of institutional integration that no single service, nation, or doctrine can achieve alone. The 2021 NATO Warfighting Capstone Concept (NWCC) formalises this vision, establishing MDO as the Alliance's primary conceptual response to the challenge of operating across contested domains at the required speed.[4] The synchronization of non-military activities alongside military ones reflects NATO's broader commitment to human security[5]: ensuring that the protection of civilians and the preservation of governance structures are embedded in operational planning from the outset, not treated as post-conflict afterthoughts.[6]

The shift toward MDO has also accelerated a process that was already underway: the distribution of capability-development responsibilities to partner nations. As adversaries employ Anti-Access/Area Denial (A2/AD) strategies, cyberattacks, and space-based threats to complicate NATO's freedom of manoeuvre, the Alliance can no longer afford partners that are effective only in conventional land operations. The requirement for partners to contribute across domains — or, at minimum to avoid creating exploitable vulnerabilities within them — drives the evolution of SFA from a training-focused activity toward a broader institutional reform enterprise.

[3]NATO Allied Command Transformation, Multi-Domain Operations: Enabling NATO to Out-Pace and Out-Think Its Adversaries.
[4]NATO 2021, Allied Command Transformation, NATO Warfighting Capstone Concept (NWCC).
[5]NATO Allied Command Transformation, Multi-Domain Operations Explained.
[6]NATO 2024, Science and Technology Organization, STO-TR-HFM-ET-201: Human Security – Frameworks, Concepts, Actors, and Challenges in Relevance to NATO.

This paper traces that evolution and identifies where doctrine, practice, and resourcing have yet to catch up with strategic need.

This paper argues that SFA must be recognised as a structural enabler of MDO rather than a supplementary activity, and that this recognition requires corresponding changes to doctrine, resourcing, and metrics of success. Without resilient and interoperable partner forces, NATO's own multi-domain effectiveness is constrained at its most critical interface: the partner nation.

The analysis is qualitative in method, drawing on doctrinal review, institutional documentation, and operational case study. Each chapter applies the MDO framework to its domain, assessing the adequacy of existing SFA practice against the demands that multi-domain integration places on partner forces and their supporting institutions. Where relevant, NATO Mission Iraq provides an operational reference point that illustrates how multi-domain pressures manifest in practice — not as the paper's sole empirical basis, but as an operationally mature mission whose institutional record makes abstract doctrinal questions concrete. The domain-specific chapters draw on their respective evidence bases.

1.2 Historical Background

The evolution from joint to MDO was not a sudden conceptual leap but a gradual accumulation of operational experience, doctrinal revision, and technological change spanning nearly a century. Understanding this trajectory matters for SFA practitioners because the principles that shaped joint doctrine — unity of command, interoperability, integrated planning

— continue to underpin MDO even as the concept moves well beyond their original scope.

The Second World War provided the first large-scale test of joint operations where coordination between different military services became a strategic imperative. The creation of Supreme Headquarters Allied Expeditionary Force (SHAEF), led by General Dwight D. Eisenhower, established the template for integrated multinational command: a single authority coordinating land, naval, and air forces across a shared strategic objective. As historian Williamson Murray has argued, these operations demonstrated that "synergy among services" is a prerequisite for success in coalition warfare, not merely an organisational preference.[7] The D-Day landings on 6th June 1944 remain the defining illustration: naval forces providing fire support and logistical lift, air forces securing the operational environment above the beaches, and ground forces executing the assault — each branch dependent on the others for the campaign to succeed.[8] Eliot Cohen has argued that this success was a product of organisational discipline as much as material superiority: the Allies' ability to coordinate complex, multi-service action under unified command proved decisive in conditions where Germany held significant defensive advantages.[9]

Not all early experiments in joint warfare produced comparable results. The Gallipoli campaign of 1915 illustrated with equal clarity the

[7]Knox, M. and Murray, W. (2001). The Dynamics of Military Revolution, 1300–2050. Cambridge: Cambridge University Press.
[8]Murray, W. (1999). "Operational Art in World War II." The Journal of Military History, 63(2), pp. 331–352.
[9]Cohen, E. and Gooch, J. (2006). Military Misfortunes: The Anatomy of Failure in War. New York: Free Press.

consequences of insufficient coordination: the failure to synchronise naval and land operations led to tactical incoherence, logistical breakdown, and operational stalemate at a cost of over 130,000 Allied lives.[10] These failures directly informed the planning processes of the Second World War. Three principles emerged from this period that remain foundational to contemporary joint and multi-domain doctrine:

- **Unity of Command**: a unified command structure reduces duplication of effort and preserves decision-making coherence under pressure. This principle was foundational to SHAEF's effectiveness and remains central to modern joint and MDO architectures.
- **Interoperability**: the standardisation of equipment, procedures, and communication protocols determines whether forces from different services and nations can function together when operational conditions demand it.
- **Integrated Planning**: accounting for the capabilities and limitations of each domain from the outset — rather than improvising coordination under fire — proved decisive in Normandy and has remained a cornerstone of effective joint doctrine ever since.

The Cold War institutionalised these lessons across the Alliance. NATO's establishment of the Supreme Headquarters Allied Powers Europe (SHAPE) in 1951 embedded multinational force integration into the

[10]Rhodes James, R. (1965). Gallipoli. London: Batsford. The campaign is widely cited as the defining case study in the operational consequences of failed naval-land coordination.

Alliance's permanent architecture.[11] Harold Winton's theoretical work on joint operations during this period elaborated the concept of "operational synergy" — the idea that integrated military action generates effects exceeding the sum of individual domain contributions, because each domain's output creates conditions that amplify the effectiveness of the others.[12] Colin Gray extended this argument by observing that the foundational principles of joint operations retain their validity even as the operational environment expands into new domains; the challenge is never simply one of adding capabilities, but of sustaining the command coherence required to employ them together.[13]

The AirLand Battle doctrine, introduced in 1982, marked the decisive evolution of joint doctrine toward what would eventually become MDO.[14] Designed to offset Soviet numerical superiority in Europe, it moved beyond linear attritional warfare by targeting enemy rear-echelon forces, logistics networks, and command-and-control structures simultaneously with front-line engagements. Its core tenets — depth, agility, initiative, and synchronisation — prioritised operational tempo over positional advantage, compelling adversaries to defend across a wider and less predictable area than they could sustain. The doctrine's reliance on precision-guided munitions, enhanced communications systems, and real-

[11]Kaplan, L.S. (1999). The Long Entanglement: NATO's First Fifty Years. Westport, CT: Praeger. See also: Pedlow, G.W. (ed.) (1997). NATO Strategy Documents 1949–1969. Brussels: NATO International Staff/SHAPE.

[12]Winton, H.R. and Mets, D.R. (eds.) (2000). The Challenge of Change: Military Institutions and New Realities, 1918–1941. Lincoln: University of Nebraska Press.

[13]Gray, C.S. (1999). Modern Strategy. Oxford: Oxford University Press.

[14]U.S. Army Training and Doctrine Command, FM 100-5 Operations (1982). Fort Monroe, VA: TRADOC.

time intelligence represented the beginning of a deep intertwining of military effectiveness and technological integration that has only intensified since.

AirLand Battle's limitations became apparent within a decade of its introduction. Its architects had designed it for a peer conventional adversary with predictable force structures and geographic boundaries. It offered no conceptual framework for asymmetric threats, information operations, or the growing influence of non-conventional domains. By the late 1990s, the rise of hybrid tactics and adversary integration of cyber and electronic warfare capabilities had exposed these gaps.[15] The doctrine's implicit assumption that land-air integration was sufficient for operational success became untenable as the operational environment expanded horizontally into space and cyberspace, and vertically into the information and cognitive domains.[16] [17]

The post-Cold War period accelerated this expansion. GPS, satellite communications and digital networks became load-bearing infrastructure for both civilian society and military operations, creating dependencies that adversaries were quick to exploit. Russia's cyber campaigns in the early stages of its aggression in Ukraine demonstrated the operational consequences: targeted disruptions to communications infrastructure could isolate ground forces and undermine civil-military coordination without a single kinetic strike. NATO's recognition of cyberspace as an operational

[15]Watling, J. and Roper, D. (2019). European Allies in US Multi-Domain Operations. London: Royal United Services Institute.

[16]Caprio, L. et al. (2020). NATO Multi-Domain Operations: Challenges for the European Land Forces. Brussels: FINABEL.

[17]NATO Science and Technology Organisation, STO-TR-HFM-ET-201 — see footnote6.

domain in 2016 acknowledged a strategic reality that military planners had been grappling with for years.[18] Space followed a parallel trajectory. Navigation, timing, communications, and intelligence collection had long depended on satellite infrastructure, but the assumption of uncontested access persisted far longer than the evidence warranted. China's development of anti-satellite weapons and its deployment of BeiDou as a strategic alternative to GPS signalled the militarisation of an environment that NATO had treated as a permissive commons.[19] [20] NATO's formal recognition of space as an operational domain in 2019 acknowledged both the Alliance's strategic dependence on space-based services and its inability to take continued access for granted.[21] [22]

1.3 Joint Operations vs Multi-Domain Operations

The cumulative effect of these domain expansions — and the interdependencies, vulnerabilities, and actors they introduced — is precisely what makes the distinction between joint operations and Multi-Domain Operations a substantive one, not a terminological update.

[18]NATO 2016, Warsaw Summit Declaration, para. 70.
[19]NATO 2018, Brussels Summit Declaration, para. 57.
[20]Tejinder Singh (2024). "Evolution of Multi-Domain Operations and Prospects for Application of Aerospace Power." Journal of Defence Studies, pp. 70–73.
[21]Royal United Services Institute (RUSI) (2019). European Allies in US Multi-Domain Operations, pp. 12–14 — see footnote 15.
[22]NATO 2022, AJP-3.20, Allied Joint Doctrine for Cyberspace Operations.



Figure 1: MDO is not the sum of the different domains

Joint operations were developed to ensure that the different branches of the armed forces could function cohesively in combat, reducing inefficiencies and enabling coordinated planning across services. The approach achieved its design objectives in the environments for which it was conceived. Its limitations emerged not from doctrinal failure, but from changes in the operational environment which it was never designed to address: the emergence of space and cyberspace as contested domains, the growing role of non-military actors in shaping outcomes, and the persistence of conflict activity well below the threshold of conventional hostilities.

MDO does not supersede joint doctrine — it builds upon it. The distinction lies in the depth of integration required and the level at which that integration must occur. Under joint doctrine, each service component contributes within its domain, coordinating with others through a hierarchical command structure that preserves a degree of operational independence. MDO demands convergence: effects across domains that are designed and synchronised from the outset rather than deconflicted after the fact. An initial reading might suggest that MDO is simply the sum of the traditional domains — land, maritime, and air — plus the newer ones of space and cyber. This is a common but misleading interpretation.

The difference between adding domain capabilities and integrating them is not semantic. When a cyber effect is synchronised with a precision strike

to degrade an adversary's command and control at the precise moment when it is most needed, the combined result exceeds what either effect would produce independently. The formula in Appendix 1 represents this mathematically: MDO effectiveness is a function of cross-domain interaction coefficients, not a simple aggregate of individual contributions. When one domain is degraded — when cyber networks are disrupted or space-based services denied — the interactions that generated the surplus collapse, and the loss is proportionally greater than the isolated contribution of the degraded domain. This is what makes MDO both more powerful and more fragile than joint operations.

$$MDO = \left(\sum_{i<j} k_{ij}(X_i \cdot X_j) \right) \times K_{sync}$$

$\mathbf{X_i}$, $\mathbf{X_j}$: Military domain capabilities
$\mathbf{k_{ij}}$: Interaction between domains (0 to 1)
$\mathbf{i < j}$: Domain pairing condition
$\mathbf{K_{sync}}$: Military-nonmilitary synchronization (1 to 2, increasing effect)

Figure 2: MDO interaction formula. Further details in Appendix 1

The integration of non-military actors reinforces this asymmetry. Commercial satellite communications, private cybersecurity infrastructure, and civilian data networks are embedded within modern military operations rather than peripheral to them. The conflict in Ukraine has demonstrated this concretely: Starlink's role in sustaining Ukrainian

command and control in 2022 showed that operational continuity in contested environments could depend on a private company's commercial decisions rather than on sovereign military capability. Under joint doctrine, such actors remain external partners. Under MDO, planning for their involvement — including the risks of their withdrawal — is not optional.

The most consequential shift that MDO introduces is from a sequenced, phase-based model of operations to persistent, cross-domain competition. Adversaries shape the battlespace continuously through cyber intrusions, disinformation, economic coercion, and grey-zone activity — long before any formal threshold is crossed. MDO provides a framework for responding to this reality: one in which the ability to generate effects across domains simultaneously, at speed and with precision, determines whether the Alliance can stay ahead of threats that are specifically designed to remain below the level that would trigger a conventional response.

NATO's MDO approach accordingly moves away from viewing operations through the prism of individual component commands and their established capabilities. Instead, it focuses on generating complementary effects across interconnected domains, imposing dilemmas on adversaries who must now defend simultaneously across multiple dimensions. The pressure this creates is not simply additive — it compounds, straining adversary decision cycles and revealing exploitable vulnerabilities that single-domain approaches never expose.

1.4 Concept and Objectives of SFA

SFA is defined in AJP-3.16 as the set of activities that support the development of the capacity and capability of foreign security forces and their supporting institutions. The definition is deliberately broad, encompassing training, advising, mentoring, equipping, and the institutional development work that enables partner forces to sustain capability independently over time. Within the MDO framework, this breadth reflects the operational reality that building a partner force capable of functioning in a multi-domain environment requires changes that go well beyond tactical training programmes.

NMI offers a concrete illustration of this distinction. Established in 2018 at the Iraqi government's request, NMI does not conduct combat operations. Its work — advising on defence planning, reforming military education, strengthening logistics systems, and embedding governance principles across the Iraqi security sector — is designed not to produce immediate tactical results but to create the institutional foundations that make tactical effectiveness sustainable over time. This is precisely the shift that MDO demands of SFA: from capability transfer to capability generation from within. The NMI case is examined in depth in Chapter 3.

What makes NMI relevant to MDO is not its technology footprint but its conceptual orientation. The mission operates in an environment shaped simultaneously by hybrid threats, cyber intrusions, information manipulation, regional power competition, and climate-related pressures — all of which act across multiple domains. Advisory work on defence planning must therefore account for threats that do not arrive through a

single domain. Cyber defence was included in the original 2015 Defence Capacity Building package for Iraq precisely because the institutional vulnerabilities that enable successful cyber intrusions — poor information governance, inadequate training, absent incident response procedures — cannot be addressed by technical means alone. SFA, in this sense, is the instrument through which MDO's cross-domain logic is translated into institutional practice at the partner level.

This reframing carries direct implications for how SFA programmes are designed and assessed. A training mission that focuses narrowly on tactical proficiency may produce forces that are locally effective but interoperably fragile — forces that cannot integrate into NATO-led operations, cannot protect their own networks, and cannot sustain their capability when external advisory support withdraws. The appropriate standard of measurement is not immediate tactical performance but institutional resilience: the degree to which partner forces can identify threats across domains, make decisions at the right level and speed, and sustain operations without external dependency. This is a more demanding objective. It is also the only one that makes SFA a genuine and durable contributor to Alliance deterrence rather than a recurring expenditure that generates diminishing returns.

Interoperability — technical, doctrinal, and cultural — remains the mechanism through which SFA generates effects at Alliance level. Partner forces that share common command-and-control architectures, reporting formats, and decision-making processes can be integrated into NATO operations without the delays that incompatible systems impose. In an MDO environment, interoperability extends beyond the procedural: it

requires that partner forces understand the cross-domain dependencies shaping the environments they operate in, and that they can contribute to — or at minimum not compromise — the multi-domain effects that NATO generates around them. Building that understanding, at the institutional level and over time, is what SFA in the context of MDO ultimately requires. Finally, Appendix 2 complements the analysis with a practical project management toolkit for the planning, governance and assessment of SFA delivery in multi-domain settings, while Appendix 1 provides the formal representation of the multi-domain interaction logic on which this paper's argument rests.

Chapter 2 — Climate Change Considerations

Of all the challenges that define the contemporary operational environment, climate change is singular in one respect: it does not act within a single domain but across all of them simultaneously. It degrades the physical infrastructure on which military operations depend, compresses training windows, accelerates resource competition, and generates the governance fragility and population displacement that create the conditions which SFA missions are designed to address. In this sense, climate change is not a thematic addition to an analysis of SFA in MDO — it is a structural condition that shapes every domain examined in the chapters that follow.

That is why this paper addresses it before turning to the domain-specific analysis. Land, maritime, air, space, and cyber operations do not unfold in a stable physical environment that can be treated as a constant. They unfold in an environment that is itself changing — and that change has direct consequences for how SFA is designed, delivered, and assessed. Partner forces that are trained and equipped without accounting for climate-driven disruption may be effective today and inadequate tomorrow. Recognising SFA as a structural enabler of MDO therefore requires, as a first step, recognising climate change as a structural condition of the environment in which MDO takes place.

The contribution that follows was developed by the NATO Climate Change and Security Centre of Excellence (CCAS COE).

It examines the operational consequences of climate change through a three-level analytical framework — distinguishing between primary environmental disruptions, secondary resource and infrastructure impacts, and tertiary socio-political effects — and identifies where these consequences intersect with SFA planning, training, and capability development. The analysis provides the environmental baseline against which the domain-specific chapters of this paper should be read.

Impact of Climate Change on the Operating Environment and the Consequences for SFA

Lt. Col. Gianfranco Pino (ITA-Carabinieri), Author
NATO Climate Change and Security Centre of Excellence (CCASCOE)
Head of Standardization, Concept Development & Experimentation Branch (SCD&E)

Dr. Emil Havstrup, Reviewer
NATO Climate Change and Security Centre of Excellence (CCASCOE)
Concept Development & Experimentation Officer

2.1 Introduction

Climate change is leading to a rise in global average temperatures and a shift in climate patterns, increasing the frequency and intensity of natural disasters and extreme weather events.[23] These developments have major repercussions for military logistics, operations and strategy, as this instability disrupts previously reliable climatic conditions and requires militaries to invest in adapting to new realities.[24] NATO has recognized these challenges and has taken proactive steps in integrating climate considerations into its strategic planning. The establishment of the NATO Climate Change and Security Centre of Excellence[25], based in Montreal, exemplifies the growing institutional commitment to addressing the

[23] IPCC, Climate Change 2022: Impacts, Adaptation and Vulnerability, Chapter 16: "Key Risks across Sectors and Regions".
[24] Van Schaik, L. et al., Ready for Take-off?: Military Responses to Climate Change (2020).
[25] NATO 2023, Climate Change and Security Agenda.

security implications of climate. The COE is aimed at addressing knowledge gaps in the nexus space between climate and security, helping to inform other branches of the armed services on how to adapt and mitigate their activities in light of these developments. This is particularly important in relation to the field of SFA operations as they are primarily focused on transferring knowledge and lessons learned to partner nations and their security forces. SFA is, therefore, a critical component in NATO's efforts to ensure that the Alliance has the institutional knowledge and capacity to maintain a high level of readiness in the decades to come. With this chapter, we highlight how the SFA COE can incorporate climate security considerations into their efforts in training, mentoring, assisting, equipping and enabling partner nations. Furthermore, we identify entry points where the field of SFA can benefit from considering the security implications of climate change and can ensure that military planners, policymakers and security professionals have the guidance needed to navigate an ever-evolving landscape.

2.2 Effects of Climate Change

Climate change is a human induced phenomenon driven by the emission of greenhouse gases (GHGs), such as carbon dioxide (CO_2) and methane (CH_4),[26] from human activities that include transportation, construction, agriculture and land-use change, among others.[27] These emissions remain in the Earth's atmosphere and absorb and re-radiate infrared heat emitted

[26] Council on Strategic Risks 2024, NOAA State of the Science Fact Sheet: Solar Radiation Modification.
[27] NASA 2020, The Causes of Climate Change.

from Earth, thus preventing it from dissipating into space and raising average global temperatures as more energy is retained on the planet. These associated rising temperatures destabilise Earth systems upon which we depend leading to increased periods of intense heat, prolonged periods of drought, melting of permafrost and glaciers, sea level rise and erratic weather patterns. These effects directly impact the resilience of communities across the globe and exacerbate existing security and social issues, acting as a threat multiplier that amplifies factors such as violence, poor governance and resource scarcity.[28] While an agreed definition of climate security is still being developed, it can be characterized as how climate-related risks impact environmental sustainability,[29] human safety[30] and societal stability.[31] This definition underscores the interconnection between climate change and security dynamics, highlighting the necessity of integrating climate resilience into strategic military and policy

[28] Goodman, S., 2024 Threat Multiplier: Climate, Military Leadership, and the Fight for Global Security.

[29] Climate change directly affects natural systems, such as water cycles, biodiversity, and agriculture, which in turn threaten environmental stability. The degradation of these systems can lead to resource scarcity, which may fuel tensions over access to essential resources like water and food.

[30] Extreme weather events, sea-level rise, and changing climate patterns pose direct threats to human life and health. Disasters such as floods, heatwaves, and hurricanes not only cause immediate harm but also exacerbate existing vulnerabilities, especially in marginalized communities. These hazards can lead to displacement, increasing the risk of human rights violations, health crises, and social unrest.

[31] As environmental conditions worsen, climate change can act as a "threat multiplier," amplifying pre-existing social, political, and economic tensions. Resource competition, migration pressures, and the displacement of populations can exacerbate conflict, destabilizing regions and, in extreme cases, leading to violent clashes. Societies with weaker governance structures or those already facing conflict are often the most vulnerable to the security threats posed by climate change.

frameworks and emphasising how environmental shifts are not isolated but rather interlinked with social, political, and economic factors.

These effects of climate change can be divided into three categories: primary, secondary and tertiary,[32] each of which impacts the operational environment of armed forces in profound ways.

The **first** and most direct impact of climate change is environmental disruption such as extreme weather events, sea level rise, floods, thawing permafrost, and increased temperatures. These effects have repercussions across multiple systems, not only leading to crop failures, water shortages and increased vulnerability to disease outbreaks,[33] but also putting critical infrastructure at risk (damaging roads, buildings and power grids) and compromising military readiness.

Primary impacts have immediate repercussions on the safety of troops and the integrity of military installations. Recent studies highlight the vulnerability of key military bases, particularly in coastal regions such as Norfolk, Virginia, where recurrent flooding poses operational challenges.[34] The U.S. Department of Defense alone has identified over 1,700 military installations at risk from climate-related hazards, underscoring the scope of this challenge.[35]

While the primary effects are an immediate and visible environmental change, the **secondary effects** are the direct consequences that stem from

[32]IPCC, Climate Change 2022: Impacts, Adaptation and Vulnerability.
[33] Skevaki, C. et al., 2024 "Impact of Climate Change on Immune Responses and Barrier Defense," Journal of Allergy and Clinical Immunology.
[34] Lopez, C.T., 2021 "DOD, Navy Confront Climate Change Challenges in Southern Virginia," U.S. Department of Defense News.
[35]Congressional Research Service 2019, Military Installations and Sea-Level Rise.

primary climate impacts. These effects arise from the disruption of essential resources such as access to land and livelihood, food, water and energy. Their repercussions are felt across multiple sectors such as agriculture, infrastructure, public health and biodiversity.

Tertiary effects extend beyond the immediate environmental and resource-based impacts and focus on the broader socio-political consequences; they are usually defined as the long-term effects of the primary effects. These consequences manifest themselves as systemic disruptions which are linked to population displacement, weak governance, territorial disputes over resources, and extremist recruitment that exploits climate-induced grievances. In discussing tertiary effects, we are essentially addressing the combined impact of the primary and secondary effects on geopolitical stability.

SFA operations should account for such drivers in the types of training they provide for partner nations. This will help to build resilient security forces that are capable of responding to both conventional and non-conventional security threats that arise in grey zone or sub-threshold conflict environments.

2.3 How Climate Change Impacts the Operational Environment

Climate change has introduced new uncertainties and challenges for military operations and thus offers an opportunity to rethink how SFA missions are conducted.

While traditional operations rely on predictable environmental factors, climate instability now requires a thorough revision of the strategies and

capabilities of security forces to effectively adapt to an unpredictable operational environment.[36]

It is important to highlight how climate change also produces tangible and immediate effects also on the operational capabilities of the armed forces. Some of these impacts include:[37]

- reduced training windows: extreme weather events, such as wildfires or floods, shorten the time available for personnel training, affecting operational readiness;
- accelerated equipment wear and tear: harsh climatic conditions increase maintenance needs and accelerate the obsolescence of military equipment and vehicles;
- personnel health and well-being: new environmental conditions pose challenges to the physical and mental health of military personnel, requiring new forms of support and adaptation;
- force redesign: armed forces must rethink their organisational structures and resource distribution in light of emerging environmental and geographic realities.

To address these challenges and respond dynamically in unpredictable operational environments, NATO is increasingly enhancing Allied awareness and understanding of the impacts of climate change on security, to inform its adaptation to the evolving strategic and operational environment and ensuring that climate-related risks are considered across

[36]NATO 2021, NATO Climate Change and Security Action Plan.
[37] CNA Military Advisory Board 2014, National Security and the Accelerating Risks of Climate Change.

land, sea, air, space, and cyberspace domains.[38] This involves both upgrading existing infrastructure and mobile equipment to ensure that bases are able to cope with climate stress factors, and raising awareness and sharing information among Allied troops on the risks that climate change poses to their respective operations. Allied and partner nation officers should be able to identify how climate change may affect them in a given situation and take into account the unpredictability brought about by climate change in their planning and execution of orders. The NATO Climate Change and Security Action Plan establishes a clear framework for how the Alliance can increase Allied awareness, adapt to climate change, mitigate their respective impact, and enhance outreach among partners[39]. SFA could contribute substantially to the first and fourth points. In particular, to strengthen training, it could make good use of case studies relating to climate change impacts to strengthen their training activities. For example, flooding and extreme weather in land and sea domains can disrupt transport routes, making logistical operations and troop movement difficult. Devastation of infrastructure is often seen in natural disaster zones, as demonstrated in the aftermath of the 2015 Nepal earthquake,[40]

[38] An example of NATO's efforts is the research to develop drones capable of operating in the Arctic's extreme conditions, including freezing temperatures, ice, and fog from Reuters, "NATO Scrambles Drones That Can Survive Arctic Conditions" (2025).
Furthermore, in July 2024, NATO released its third edition of the report "Climate Change and Security Impact Assessment", which examines the impact of climate change on each of NATO's operating domains – sea, land, air, space and cyber – as well as on NATO's missions and operations, and resilience and civil preparedness. NATO, Climate Change and Security Impact Assessment (2024).
[39] NATO Climate Change and Security Action Plan, 2021. U.S. Indo-Pacific Command, Nepal Earthquake Relief Effort Named Operation Sahayogi Haat (2015).
[40] In the 2015 Nepal earthquake military operations played a crucial role in both recovery efforts and providing logistical support.

where successive flooding compounded the difficulties of humanitarian and military operations; other examples include the effects of the extreme weather events that occurred in Myanmar in 2008[41] and in Puerto Rico in 2017.[42] SFA training could pass on lessons learned from examples such as these to facilitate a passing on of institutional knowledge.

2.4 Adapting Security Forces to Climate Change: Challenges, Multilateral Approaches and Capability Development

The challenges posed by climate change undoubtedly necessitate a significant adaptation of SFA efforts, especially in empowering partner security forces to manage environmental crises and resource-related conflicts. The integration of military, humanitarian and development efforts will continue to be essential in building a comprehensive approach to these challenges. Force development priorities should shift to accommodate these evolving needs, with military capabilities revised to

[41] Cyclone Nargis struck Myanmar in early May, causing widespread devastation. It was one of the deadliest tropical cyclones ever recorded, killing an estimated 138,000 people. The storm caused severe flooding, destroyed homes and disrupted agriculture, particularly in the Irrawaddy Delta region. Military forces were instrumental in rescue operations and the distribution of aid to those in need. The Guardian, "Regime Blocked Aid to Burma Cyclone Victims" (2009).

[42] On Sept. 20, 2017, Puerto Rico was hit by the deadliest U.S.-based natural disaster in the last 100 years, according to NBC News. Hurricane Maria had the highest average rainfall of all 129 storms that have hit Puerto Rico in the past 60 years, according to the American Geophysical Union. The hurricane dropped around 41 inches (104 centimetres) of rain onto the island, which caused devastating floods. Research published in the New England Journal of Medicine estimated that the total death toll caused by Hurricane Maria was more than 4,600. It was the third most costly tropical cyclone in the U.S., causing around $98 billion worth of damage, according to the National Oceanic and Atmospheric Administration (NOAA). Military operations were vital to the rescue and recovery efforts, ensuring that aid reached the affected population.

include specialised equipment for extreme weather operations, sustainable logistics to minimise environmental footprints, enhanced medical readiness for climate-related health threats, and stronger mechanism for civil-military coordination mechanisms. This section highlights how SFA could benefit from a more multilateral approach alongside a revamp of training to integrate climate security into its programming.

2.4.1 A Multilateral Approach

SFA could benefit from integration into a multilateral approach involving local, regional and international actors. Partner security forces are, and will be, called upon not only to defend territory but also to manage and resolve social and political conflicts that may in part be driven by environmental insecurity. Addressing climate linked drivers of conflict will require targeted interventions and programmes that address socio-economic inequalities, resource scarcities and poor governance. Security forces will have a part to play in enabling these initiatives and providing a security guarantee for societies that are destabilised by the climate change. SFA efforts will be critical in providing partner nations with the institutional capabilities to understand climate sensitivities. This can help to address the root causes of conflict and enable more resilient societies.

2.4.2 Training Programmes for SFA Units

To tackle the evolving challenges posed by climate change, training programmes for both security forces and SFA units should place greater emphasis on key areas such as climate security, environmental awareness, adaptability, and cross-functional skills. Forces with diversified skill sets will be more effective in climate-affected environments. This emphasises

the need to update traditional training curricula to include multi-domain competencies which could encompass knowledge of climate and environmental security, including the protection of natural resources.

Current SFA training programs could benefit from a specific focus on climate-related issues, given that local forces may lack proper training in managing natural disasters (e.g., floods, wildfires or droughts), which are becoming more frequent due to climate change. Regarding possible modules which could be integrated into SFA training programmes, a long list of subjects could be recommended for consideration, such as: *climate security awareness, climate change adaptation strategies, environmental monitoring and protection, disaster response and civil-military coordination, MDO in changing climate, technological integration and interagency international cooperation.*

To close training gaps and create a practical, dynamic learning experience that prepares security forces for the unpredictability of climate change-related challenges, it would be beneficial to engage participants in exercises based on possible scenarios simulating climate crises, resource conflicts, or maintaining security during environmental disasters. These exercises could be further enhanced with wargaming techniques, allowing participants to engage in strategic decision-making simulations that would test their ability to adapt to evolving conditions and tackle complex threats.[43] Addressing climate challenges will require not only adapting security force training but also integrating new technologies, such as drones and robotics, into SFA activities.

[43] Cameron, A. and Burke, S. (2022) "Wargaming Climate Change: Who Plays for the Red Team?" War on the Rocks.

2.5 Conclusion

Climate change is significantly reshaping the operational environment of armed forces, particularly in SFA missions. As previously discussed, the effects of climate change, are transforming the global security landscape, requiring an adaptation of security strategies. SFA missions, in particular, will need to evolve to address not only conventional threats but also environmental, socio-political, and economic challenges related to climate change. This is due to the ability of climate change to act as a threat multiplier and a catalyst for instability and conflict, in tandem with more conventional threats. The growing climate uncertainty will require ever-increasing strategic planning that considers environmental vulnerabilities, promoting timely and coordinated actions to reduce operational risks and enhance military preparedness. In the context of SFA missions, it will be crucial to develop capabilities to respond to environmental crises, such as strengthening the protection of natural resources, managing migration flows, and safeguarding vital resources in conflict or disaster scenarios.

It would be beneficial for SFA missions to involve specialists in climate security and environmental protection for the purposes of their training. These training can help to strengthen coordinated responses across different branches of service and operational domains. They would also allow for the maintenance and expansion of institutional knowledge and facilitate the exchange of information between scientific and military communities. Some NATO member states have already implemented such

training within units,[44] and recently, the NATO Political Committee has discussed the possibility of establishing a NATO Climate Change Advisor role.

By integrating climate security considerations into the training provided to security forces the SFA COE can significantly enhance the ability of partner nations to operate effectively in the face of climate-related challenges. A significant achievement would be to ensure that the curricula for our soldiers incorporate specific modules on climate change, which should be regularly updated to reflect advancements in research and emerging best practices. Climate factors should be viewed as a central component of both strategic and operational planning, rather than as secondary concerns or an unforeseen event. This requires a shift in perspective to fully recognise their significance. The CCASCOE is already working to integrate climate change considerations into NATO doctrines, helping to drive this shift.

Ultimately, the evolution of SFA operations should carefully consider the increasing complexity of climate-related challenges. Adapting armed forces to climate change is not only an operational necessity but a strategic priority to ensure long-term global security.

[44] Pérez, V. et al., (2022) "Expanding the New Roles of the Military – The Case of Spain's Military Emergency Unit: A Research Note," Armed Forces & Society.

Chapter 3 — Land Domain

The land domain is the most thoroughly documented dimension of SFA. NATO doctrine — from AJP-3.16 to AJP-3.2 — provides an extensive framework for land-based SFA, and the academic literature on training, advising, and capacity building in ground operations is well established. This accumulated body of knowledge reflects a deeper truth: it is in the land domain that populations live, governments exercise sovereignty, and the legitimacy of the state is built or eroded. Whatever else modern conflict involves, its political outcomes are ultimately determined on the ground. This is why the land domain remains the foundation of NATO's collective defence posture, and why SFA in this dimension has historically received the greatest doctrinal and operational investment. This chapter does not attempt to reiterate those foundations.

What is less well understood is how land-centric SFA performs when the operational environment can no longer be treated as exclusively terrestrial. In an MDO framework, the land domain does not disappear — it anchors the other domains — but it is simultaneously exposed to pressures from the cyber, information, space, and cognitive dimensions that directly shape what happens on the ground. Adversaries who cannot match NATO in conventional land power have learned to exploit these lateral pressures: degrading communications, manipulating information environments, and exploiting governance vacuums to undermine the institutional foundations that SFA is designed to build. Therefore, the question this chapter addresses is therefore not what SFA in the land domain looks like in general, but how it adapts — structurally, doctrinally,

and institutionally — when that ground is simultaneously contested across multiple dimensions simultaneously.

NMI answers that question with operational evidence accumulated over more than six years. As NATO's only enduring capacity-building mission in the Middle East, NMI has advised Iraqi security institutions in precisely this kind of environment: one shaped simultaneously by hybrid threats, information manipulation, cyber intrusion, regional power competition, and the long-term pressures of climate-driven instability. It is a mission that operates in the land domain but cannot be understood through the land domain alone. The analysis that follows, developed by Col. Aurelio Tassi, examines how NMI's structure, objectives, and operational record illuminate what SFA as a structural enabler of MDO requires in practice — and where the gap between current doctrine and operational reality remains open. A project-level illustration of how NMI capacity-building activities are planned, governed, and sustained in practice is provided in Appendix 2, which analyses an NMI support project to the Iraqi Military Medical School through the lens of international project management standards.

As of July 2026, following a March 2026 decision, NMI continues its mission from Allied Joint Force Command Naples, having relocated from Baghdad in response to the regional security situation.

NATO Mission in Iraq: A Case Study

Col. Aurelio Tassi (ITA-Army), Author
NATO Mission Iraq (NMI)
Former Head, Specialised Programmes Coordination Office (SPCO)

3.1 Preamble

NMI focuses on Defence and Related Security Capacity Building (DCB) efforts and embodies the Alliance's strategic ambition to project stability beyond its borders through a comprehensive, multi-domain approach.[45] [46] Established at the request of the Iraqi government, NMI is designed to strengthen Iraq's security institutions and help build self-sustaining national defence structures.[47] Unlike crisis-response missions that are focused on short-term stabilisation, NMI emphasises long-term institution-building, aligning its activities with the broader frameworks of Security Sector Reform (SSR) and Security Sector Governance (SSG).[48] [49] This focus reflects NATO's recognition that fragile states are not stabilized through military means alone, but by embedding governance principles, such as accountability, inclusiveness and the rule of law, into their defence sectors.

In this sense, NMI is not only a mission in Iraq but also a strategic laboratory where NATO's evolving approach to SFA in an MDO

[45] NATO 2018, NATO Mission Iraq Established at Brussels Summit.
[46] NATO 2025, NATO Mission Iraq. NATO website.
[47] NATO, NATO Mission Iraq Established, op. cit.
[48] DCAF 2022, Geneva Centre for Security Sector Governance. Security Sector Reform: Applying the Principles of Good Governance to the Security Sector."
[49] Jackson P. (2018). Introduction: Second-Generation Security Sector Reform. Journal of Intervention and Statebuilding, Vol. 12, No. 1, pp. 1–10.

environment is being tested and refined.[50] By integrating land, air, cyber, and information dimensions into its advisory and capacity-building work, NMI supports Iraq in addressing both immediate security threats and the long-term challenges posed by regional instability, hybrid tactics, and peer competitors' influence.[51] This dual orientation - tactical effectiveness and institutional resilience - marks the mission as a cornerstone of NATO's southern flank strategy.

3.2 Strategic-Political Context

SFA in the land domain plays a pivotal role in NATO's approach to MDO. While modern warfare increasingly integrates effects across land, air, maritime, cyber, and space, the land domain remains the decisive environment for establishing political outcomes and ensuring stabilization. It is in the land domain that populations live, governments exercise sovereignty, and legitimacy is built or eroded. SFA provides the instrument for NATO to support partner nations in developing credible defence forces, particularly in the land domain, and resilient security institutions, which in turn strengthens Alliance deterrence and defence.[52] In the MDO framework, SFA contributes to synchronizing land effects with other operational domains, creating the conditions for long-term stabilization, interoperability, and partners' self-sufficiency.[53]

[50] NATO 2023, Allied Command Transformation (ACT), op. cit.
[51] Jahara Matisek & William Reno (2019). "Getting American Security Force Assistance Right: Political Context Matters." Joint Force Quarterly, No. 92, pp. 65–73.
[52] DCAF 2022, Geneva Centre for Security Sector Governance, op. cit.
[53] NATO 2023, Allied Command Transformation (ACT), op. cit.

The NMI is a significant case in point: as NATO's only enduring capacity-building mission in the Middle East, NMI demonstrates how the Alliance can operationalize MDO by linking strategic objectives, regional partnerships, and local capacity building into a coherent whole-of-society approach.[54]

The 2022 NATO Strategic Concept witnessed the first-ever participation of Asia-Pacific leaders from Australia, New Zealand, Japan, and South Korea, and reaffirmed its open-door policy, later confirmed by Sweden's and Finland's accession into NATO.[55] The NATO 2030 agenda, adopted during the June 2021 Brussels Summit, was further reinforced.[56] The most noteworthy change between the 2010 Strategic Concept and the 2022 document is the transition of Russia from being described as a "strategic partner" to NATO's "most significant and direct threat". [57] This is a direct consequence of the ongoing war in Europe between Russia and Ukraine, characterised as "the most serious security crisis" since the Second World War, which has triggered a substantial reinforcement of NATO troops along the Alliance's eastern flank.[58]

In parallel, reinforcing the 2016 NATO Warsaw Summit "Projecting Stability" agenda, NATO reaffirmed in its 2022 Strategic Concept its commitment to increasing global outreach to countries in its broader neighbourhood, by enhancing the dialogue, cooperation, and protection of

[54] NATO 2025, "NATO Mission Iraq." NATO, website
[55] NATO 2022, NATO Strategic Concept 2022. Brussels: North Atlantic Treaty Organization.
[56] NATO 2021, "Brussels Summit Communiqué." NATO, Brussels, 14 June 2021.
[57] NATO 2022, Strategic Concept, op. cit.
[58] NATO 2022, Strategic Concept op. cit.

systems, standards, and technologies on which Allied security depends. [59] In this scenario, capacity-building through capability development is bolstered across all domains to sustain reinforcement and deterrence. This implies a decisive role for NATO's armaments and associated communities in tackling the new security context.[60] Alliance-wide resilience, protection of space assets, robust cyber defences, and critical infrastructure security constitute the backbone of NATO's multi-domain posture.[61] Investments in emerging and disruptive technologies (EDTs) are increasingly essential to foster interoperability across domains and retain military advantage.[62]

In such a high-intensity, multidimensional environment, cooperation in capability development can strengthen NATO's relationships with partner nations, enhance interoperability, and encourage contributions to missions and operations[63]. Regarding the NATO–Iraq political-diplomatic relationship, NATO has been adopting a pragmatic approach to enhance cooperation with Iraqi security and military forces through NMI's capacity-building activities. [64] This mission not only consolidates NATO's footprint but also has the potential to expand into capability development and procurement partnerships.[65] NMI has been serving as a platform for consolidating relationships and leveraging defence industry opportunities,

[59] NATO 2016, NATO Policy on Countering Improvised Explosive Devices (C-IED), NATO Standardization Office.
[60] NATO 2021, "Brussels Summit Communiqué." NATO, Brussels, 14 June 2021.
[61] NATO 2023, Allied Command Transformation (ACT), op. cit.
[62] NATO 2021, "Brussels Summit Communiqué, op. cit.
[63] NATO 2023, Allied Command Transformation (ACT), op. cit.
[64] NATO, NATO Mission Iraq Established, op. cit.
[65] NATO 2025, "NATO Mission Iraq." NATO, Brussels.

intending to ensure Iraq's self-sufficiency and sustainable partnership with NATO.

3.3 Engaging with NATO Partner Nations and Relevant International Organizations

Engaging with NATO partner nations and relevant International Organizations is an essential enabler for crisis prevention, management, and long-term stabilization.[66] Within this framework, NMI has become a platform where partnerships are not abstract political declarations, but practical instruments of collective security.[67] Through the mission's direct involvement in operations, training, and Defence Capacity Building (DCB), NATO is contributing to the broader Alliance effort to mitigate instability before it escalates into open conflict, while also protecting civilian populations and civil society at large from the perpetuation of violence.[68] The consolidation of these partnerships, and their progressive involvement in SFA initiatives, deprives adversaries of space to manoeuvre and strengthens NATO's deterrence credibility in fragile regions.

The strategic value of such cooperation lies in its ability to increase interoperability and standardization - two pillars that directly enhance Alliance responsiveness and operational effectiveness.[69] Nowhere is this more relevant than in regions such as the Middle East, North Africa, and the Sahel, where NATO's presence is more limited compared to its Eastern

[66] NATO 2015, Defence Capacity Building (DCB) Package for Iraq. Brussels: North Atlantic Treaty Organization.
[67] NATO 2025, "NATO Mission Iraq, op. cit.
[68] Jahara Matisek & William Reno (2019). "Getting American Security Force Assistance Right: Political Context Matters." Joint Force Quarterly, No. 92, pp. 65–73.
[69] NATO 2023, Allied Command Transformation (ACT), op. cit.

flank, yet where instability carries equally far-reaching consequences.[70] In these contexts, SFA in the land domain emerges as the practical translation of NATO's strategic ambition to project stability through partnerships.[71] By progressively involving local actors in operational planning, capability development, and training, NATO fosters the conditions for locally owned security solutions that can prevent fragile states from degenerating into full-blown crises.[72]

Trough missions such as NMI, therefore, SFA becomes a strategic economy of force tool: by empowering local actors to address their own security challenges, NATO can extend its deterrence and footprint without the need for large-scale deployments. For instance, NATO's cooperation with Jordan and Tunisia in the DCB framework has provided valuable experience in counter-terrorism capacity building that complements the Iraqi case.[73]

A key challenge in these regions remains the populations' often negative perception of NATO, which is linked to past interventions and the influence of other great powers and international organisations.[74] NMI contributes to addressing this credibility gap by demonstrating NATO's ability to deliver non-combat, partner-focused, and demand-driven support.[75] Through careful alignment with Iraqi priorities, NMI shows that

[70] Jackson P. (2018). "Introduction: Second-Generation Security Sector Reform." Journal of Intervention and Statebuilding, Vol. 12, No. 1, pp. 1–10.
[71] NATO 2015, Defence Capacity Building (DCB), op. cit.
[72] DCAF 2022, Geneva Centre for Security Sector, SSR Backgrounder Series, op. cit.
[73] NATO 2015, Defence Capacity Building (DCB), op. cit.
[74] Jackson P. (2018), op. cit.
[75] NATO 2025, "NATO Mission Iraq, op. cit.

NATO can provide responsive and coherent assistance that respects sovereignty while enhancing stability.[76]

Within the wider framework of SSR, SFA in the land domain is effectively the modern evolution of the "boots on the ground" concept.[77] While traditional doctrine emphasized the necessity of physically deploying ground forces to control territory, modern MDO require a broader perspective: it is not enough to win battles; it is essential to shape sustainable political-military settlements.[78] In this sense, SFA replaces the



Figure 3: Relevant NATO partnership and their logos: IOs, International missions and programs

old logic of presence with the more durable logic of empowerment, providing the host nation with the expertise, institutional resilience, and doctrinal alignment required to consolidate gains across all domains.[79] The mission also illustrates how NATO integrates external actors, such as the

[76] DCAF 2022, Geneva Centre for Security Sector Governance, op. cit.
[77] Jahara Matisek & William Reno (2019), op. cit.
[78] NATO 2023, Allied Command Transformation (ACT), op. cit.
[79] Jackson P. (2018), op. cit.

United Nations (UN), European Union (EU), and regional organisations, into a cooperative framework.[80] For example, NATO advisors have coordinated with the EU Advisory Mission in Iraq (EUAM Iraq) to avoid duplication and ensure complementary support in areas like rule of law and civil-military planning.[81] Similarly, coordination with the UN Development Programme (UNDP) has been crucial in aligning security reforms with broader governance and reconstruction efforts.[82]

Finally, NMI highlights how NATO's role in the Middle East and North Africa (MENA) must account for non-traditional threats, such as the worsening consequences of climate change, which pose measurable risks to security and stability.[83] Increased desertification, water scarcity, and internal displacement could fuel instability if not addressed. By working with Iraqi institutions to integrate resilience into security planning, NMI supports a broader MDO approach that accounts for the interconnection between environmental, political, and security domains.[84]

By advancing this vision, NATO is not only addressing local challenges but also strategically positioning itself against peer and near-peer competitors who seek influence in the same geopolitical space.[85] Building Iraq into a credible NATO partner enables the Alliance to secure a foothold at the crossroads of Middle Eastern and Mediterranean security,

[80] NATO 2025, NATO Mission Iraq, op. cit.
[81] EUAM Iraq, 2023.
[82] UNPD 2022, United Nations Development Programme. Funding Facility for Stabilization – Iraq: Annual Report 2022.
[83] NATO 2025, NATO Mission Iraq, op. cit.
[84] NATO 2023, Allied Command Transformation (ACT), op. cit.
[85] Jahara Matisek & William Reno (2019), op. cit.

reinforcing its southern flank and ensuring that future sources of instability are met with proactive, cooperative, and sustainable responses. [86]

3.4 NATO's Role in Iraq's Defence and Institutional Building

Building on years of NATO involvement in Iraq since 2004, and the endorsement of NATO's DCB initiative in September 2014 at the NATO Summit in Wales, in July 2015 Allies agreed on a DCB package for Iraq with the creation of a dedicated Trust Fund.[87] Following the invitation from the Government of Iraq, NMI was formally established in October 2018.[88] The 2015 agreement is still the reference for NATO capacity building in Iraq, through the following seven priority areas of assistance where NATO could offer the most value-added in the short term:[89]

- Security Sector Reform.
- Countering Improvised Explosive Devices (C-IED), Explosive Ordnance Disposals (EOD), demining.
- Civil-military planning support to operations.
- Cyber defence.
- Military medicine and medical assistance.
- Military training.
- Civil emergency planning and preparedness.

[86] NATO 2025, NATO Mission Iraq, op. cit.
[87] NATO 2014, Wales Summit Declaration on Afghanistan and Defence Capacity Building.
[88] NATO 2025, Mission Iraq Established, op. cit.
[89] NATO 2015, Defence Capacity Building (DCB) Package for Iraq.

In this respect, NMI represents a shift from NATO's earlier crisis-response operations to a sustained advisory and capacity-building mission aimed at institutional reform [90].

Through its three divisions and one office, NMI conducts high-level advising, education, and training in order to increase the capacity and effectiveness of the Iraqi Security Institutions and Iraqi Security Forces, primarily within the MoD and down to the Service Command Headquarters, and, since 2023, within the MoI and Federal Police[91]. NMI is also engaging with the Office of the National Security Advisor (ONSA), and the Office of the Prime Minister National Operations Centre (PMNOC).

Its structure reflects this ambition:[92]

- **Ministerial Advisory Division (MAD):** works at the strategic level with the Iraqi Ministry of Defence and the ONSA to improve governance, transparency, and policy planning.
- **Professional Security Education Division (PSE):** assists Iraq in modernising its military education system, from officer academies to staff colleges, embedding NATO standards and doctrine.
- **Training Development Division (TDD):** focuses on standardizing training curricula across the Iraqi Armed Forces, ensuring that lessons learned are institutionalized.
- **StratCom, Representation & Outreach (SCRO) Office:** manages NATO's visibility, and maintains relationships with

[90] Taylor, W. (2020). 'NATO's Shift from Crisis Response to Capacity Building: The Case of Iraq.' RUSI Journal, 165(3), pp. 34–47.
[91] NATO 2022, Strategic Concept 2022, op. cit.
[92] NATO 2021, NATO Mission Iraq: Structure and Divisions, NATO Factsheet.

International Organizations and institutional stakeholders seeking for bilateral level synergies.

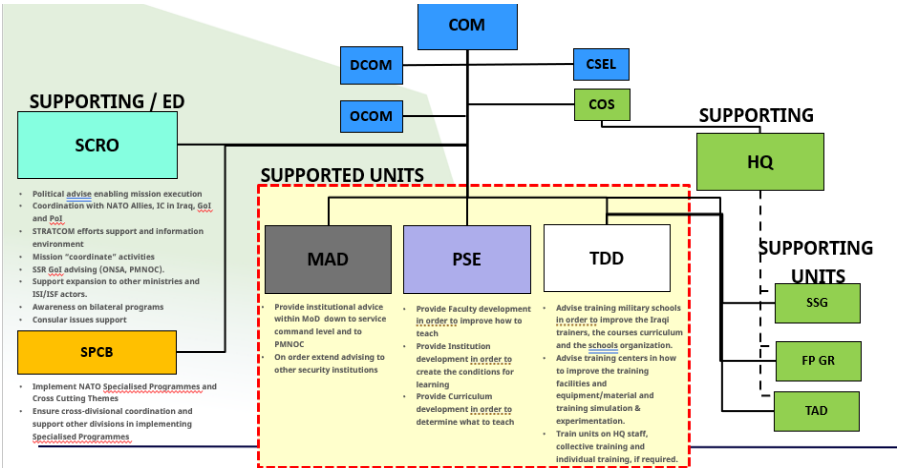


Figure 4: Diagram representing the NATO Mission Iraq (NMI)'s operational structure as a sustained advisory and capacity-building mission including the supporting and the supported units

The **Specialised Programmes Coordination Branch (SPCB)** deserves a dedicated space, due to its direct liaison authority with NATO HQ. The core function of the SPCB is to align NMI's capacity building initiatives with Allied priorities and Iraqi requirements, through bespoke DCB projects.[93] The SPCB also coordinates the implementation of NATO's partnership programmes, such as Building Integrity (BI), the Defence Education Enhancement Programme (DEEP), and NATO strategic-political cross-cutting themes such as Women, Peace and Security (WPS),

[93] NATO 2021, Specialised Programmes Coordination Branch (SPCB), NATO HQ.

Human Rights and International Humanitarian Law (HR/IHL), and Human Security (Hum Sec).[94]

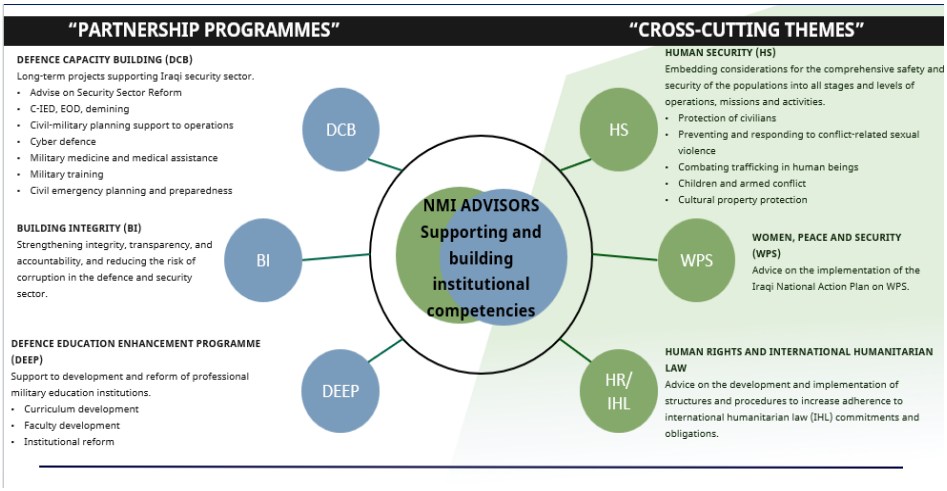


Figure 5: SPCB "toolbox" to align NMI's capacity building initiatives with Allied priorities and Iraqi requirements through the coordination of Partnership programmes and Cross-cutting themes

Breaking down to the SPCB "toolbox", each partnership programme and cross-cutting theme provides a specific perspective on the mission's goals. In particular, the BI programme consists of a voluntary, demand-driven process that provides strategic advice and capacity building, conducted with full respect for Iraq's sovereignty and territorial integrity. It provides help to Iraqi authorities in managing their defence resources effectively, preventing corruption and strengthening institutional management of defence resources, thereby helping to combat the threat of terrorism while

[94] Smith, H. (2021). 'Cross-Cutting Themes in NATO Capacity Building.' Journal of Strategic Security, 14(2), pp. 85–102.

improving integrity, transparency, and accountability within the Iraqi defence and security sectors.[95] Iraq receives tailored support through the BI Self-Assessment and Peer Review Process, a voluntary diagnostic tool that helps identify areas for reform and capacity-building. A specific instance of this was the "Building Integrity" train-the-trainers programme for the Iraqi Ministry of Defence in 2021, and the program continues to provide integrated support to the Iraqi government through NMI.

The DEEP, supports the Iraqi government's efforts to build more professional military education institutions by providing tailored, practical support to develop academic curricula and instructor capabilities.[96] This partnership focuses on areas like active adult learning methods and the promotion of continuous professional development, and involves, among to many other Allied Education Institutions, the Centre for Defence Higher Studies in Italy, the Defence Academy in the UK, and the Partnership for Peace (PfP) Consortium. The program targets key Iraqi institutions, including the Defence University for Military Studies (which houses the War College, National Defence College, and Defence Language Institute), the Education Cadre Development Centre (ECDC), and the Non-Commissioned Officers Academy. The DEEP uses a collaborative approach, providing advisory expertise to assist with curriculum

[95] Transparency International (2019). Corruption Risks in Defence and Security Sector Capacity Building. Transparency International Defence & Security.

[96] PfP Consortium (2020). Defence Education Enhancement Programme (DEEP) Handbook. Partnership for Peace Consortium of Defence Academies and Security Studies Institutes.

development, teaching methodologies, and faculty training. Key Initiatives are:

- **Faculty Development:** Developing instructor skills in student-centred, outcome-based learning.
- **Curriculum Development:** Assisting with the development and review of academic curricula to align with modern Professional Military Education (PME) standards.
- **Institutional Capability Building:** Strengthening the overall institutional capabilities of Iraqi defence education institutions.

By implementing of the cross-cutting themes such as WPS, HR/IHL, and Hum Sec, NMI ensures that the Iraqi defence and security institutions are integrating gender perspectives, protection of civilians, and inclusive, people-centred approaches in their security policies, aligned with UN Security Council Resolution 1325.[97] WPS focuses on women's equal participation and protection from gender-based violence in conflict and peacebuilding, while HR/IHL emphasises preventing and responding to the violations of international law, including gendered harm in conflict. Human Security shifts the focus from state-centric security to the protection of individuals from various threats, including those disproportionately affecting women and girls.

These three themes are deeply interconnected and mutually reinforcing. Though its advisory effort NMI is fostering a holistic approach that

[97] United Nations (2000). UN Security Council Resolution 1325 on Women, Peace and Security.

incorporates WPS and HR/IHL principles and is essential for achieving genuine and lasting human security and peace. For example, integrating a gendered perspective into civilian harm mitigation frameworks not only upholds HR/IHL but also supports women's participation and protection, thereby advancing human security.

These activities illustrate that NMI is not just about technical training but also about embedding good governance into the Iraqi security sector.[98]

To deliver on its advisory effort, NMI focuses on a number of priority areas NMI agreed with the Iraqi Security Institutions; these are called "Long-Terms Objectives (LTOs)", and they represent an "agreed co-owned methodology", setting the framework for NATO-Iraq cooperation. These LTOs are lively tools that focus on priorities and key areas and establish a clear measurable objective to achieve. To date, the areas include human resources management, security education, logistics, cyber, systematic training, development of a cadre of non-Commissioned Officers, and simulation.

But NATO's contribution in Iraq goes beyond military assistance: it aims to foster institutional resilience as the foundation of long-term security. Iraqi defence institutions, weakened by decades of conflict, corruption, and external interference, require not only better-trained forces but also more accountable and transparent systems of governance. Here, NATO's role is unique. Unlike bilateral arrangements that may focus narrowly on equipment or training, NATO engages Iraq through a holistic approach that

[98] Chuter, D. (2019). Security Sector Reform and Defense Management. Geneva: DCAF.

integrates capacity building, doctrinal development, and governance reform.

Concrete initiatives highlight this approach. The PME programmes supported by NATO are not merely about technical instruction, but about embedding democratic oversight and critical thinking into the Iraqi officer corps. Similarly, NATO's work in logistics codification enhances not just the efficiency of supply chains, but also their transparency and resilience against corruption or political manipulation. By strengthening Iraq's defence planning and resource management, NATO ensures that the Iraqi Armed Forces are not only operationally effective but also sustainable within the state's economic and political realities. Additional examples of NMI's work include supporting Iraq's National Security Strategy revision, advising on defence planning processes, and assisting in the development of Iraq's first gender integration strategy within the armed forces—reflecting NATO's commitment to UNSCR 1325 on Women, Peace, and Security[99].

This approach situates NMI at the intersection of SSR and SSG, enabling Iraq to gradually assume full responsibility for its security while fostering trust between civilian authorities and military institutions. By supporting Iraq in developing credible, accountable security structures, NATO reinforces the legitimacy of the Iraqi state, reduces the appeal of non-state armed groups, and counters the influence of external actors seeking to exploit instability. In doing so, NATO not only contributes to Iraq's sovereignty but also enhances stability across the broader MENA region.

[99] United Nations (2000). UN Security Council Resolution 1325 on Women, Peace and Security

3.5 DCB Activities in the Land Domain

DCB in the land domain is one of NATO's most visible and impactful contributions to Iraq.[100] As part of the wider SSR and SSG effort, these activities address the urgent need to professionalise the Iraqi Army and ground forces, which bear primary responsibility for controlling territory, protecting populations, and restoring state authority after years of conflict with ISIS and other armed groups. In a post-crisis scenario, rebuilding land forces is not simply a question of training tactics; it is about embedding them within a governance structures.[101]

As part of broader SSR efforts, through NMI's DCB projects NATO translates its strategic ambition into practical assistance that bridges the gap between immediate operational needs to improve tactical effectiveness and long-term institutional reform, embedding good governance principles to ensure transparency, oversight and integration with other security institutions.[102]

This double-track approach bridges the gap between the "train and equip" and long-term institution-building models, ensuring that the Iraqi security sector is both capable of responding to immediate threats and resilient enough to sustain democratic control in the long term. By anchoring reforms in SSG principles - such as accountability, inclusiveness, and

[100] NATO 2020, Defence Capacity Building in Practice, NATO Review.
[101] Donais, T. (2018). Security Sector Reform and the Challenge of Local Ownership. London: Routledge.
[102] Gaub, F. (2019). NATO's Capacity Building: Breaking New Ground. NATO Defense College Research Paper No. 150.

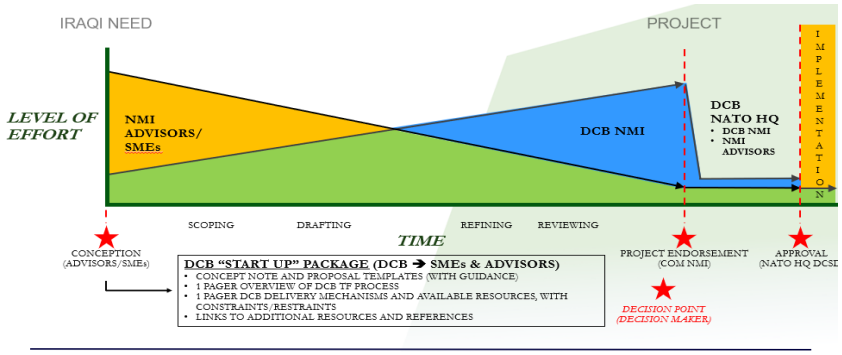


Figure 6: DCB process explaining the link between the level of effort and the timeline of the Iraqi project

adherence to the rule of law - DCB strengthens the legitimacy of Iraqi institutions while fostering interoperability with NATO standards.

In this respect, DCB activities in the land domain can be seen as the practical translation of NATO's strategic objective into project stability: they provide the tools for Iraq to move from crisis management to sustainable governance. Whether through codification of logistics systems, doctrinal reform, or PME, DCB underpins the transition from externally supported operations to nationally led security provision.

The DCB delivery mechanism relies on NATO Trust Funds and involves close coordination between NMI, NATO HQ, and international partners.[103] The process itself begins with the identification of an Iraqi defence and security capability gap or requirement, captured by NMI through any number of agents: COM NMI, advisors or subject matter experts within MAD, TDD, PSE, SCRO, or SPCB personnel, but also through different

[103] NATO 2019, NATO Defence and Related Security Capacity Building (DCB) Initiatives.

levels of interaction of NATO HQ, NATO Allies, Unified Action Partners (UAP), international community members, diplomatic networks, and various governmental and non-governmental organizations.

That gap or requirement is shared with the NMI SPCB. If the need surpasses what the relevant NMI SMEs or advisors are capable of providing organically, the NMI SME or advisor will request support from SPCB, which will screen the request and, depending on the type of gap or requirement, determine which NATO partnership programme(s) is/are best suited. The DCB process begins once DCB is determined as a suitable solution to the need or requirement identified.

Regardless of the delivery mechanism selected, NATO DCB efforts in Iraq are implemented by, with, and through NMI, and are based on a streamlined process to implement specific DCB projects. The process itself is based on the DCB Trust Fund lifecycle, and a project may be delivered through assets integral to NMI, or with the assistance of NATO assets other than NMI (e.g. IS, IMS, NMAs, NATO COEs, NATO Schools, etc.), or through international community partners who provide multilateral or bilateral assistance to Iraq.

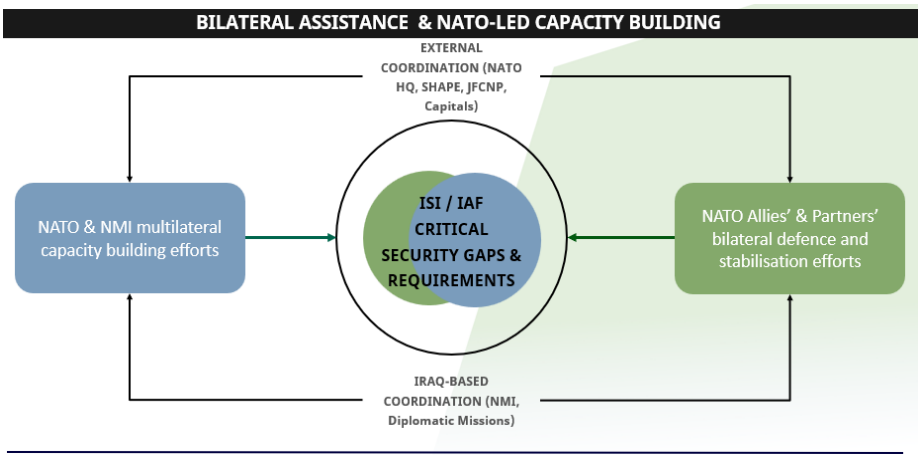


Figure 7: Representation of the bilateral assistance between external coordination and Iraq-based coordination for capacity building

Initiatives such as the implementation of the NATO Codification System (AC/135) enable Iraq to manage its logistics and procurement with greater efficiency and integrity.[104] By codifying every item - from small arms to vehicle parts - according to NATO standards, Iraq has significantly reduced corruption opportunities in procurement and improved operational readiness.

Efforts to standardize doctrine help Iraqi land forces to align with NATO practices, enhancing interoperability and creating a shared professional culture. Meanwhile, the support provided to PME institutions, spearheaded with the Iraqi Defence University for Military Studies (DUFMS) committed to reforming the defence education system, ensures that future generations of Iraqi officers are trained not only in tactics but also in

[104] NATO 2020, Codification in Support of NATO Operations (AC/135), NATO Support and Procurement Agency.

leadership, ethics, and governance principles [105]. In this respect, NATO advisors help to modernize curricula for combined arms manoeuvre and leadership development. This has measurable impact in creating a cadre of Iraqi officers trained to NATO standards, thus improving interoperability and self-reliance.

Equally, NATO support in Counter-IED (C-IED) and EOD has been critical. These programmes have strengthened Iraq's ability to confront one of its most persistent asymmetric threats, while also embedding EOD as a doctrinally recognized capability rather than an *ad hoc* solution.[106]

These projects exemplify NATO's systemic approach: institutional reforms, doctrinal development, and governance-focused capacity building rather than temporary fixes.[107]

These activities reflect the modern role of SFA in MDO. Just as "boots on the ground" were once indispensable for securing physical control, today, institution-building is indispensable for securing long-term stability. By strengthening Iraq's land domain, NATO is effectively creating the conditions for the Iraqi Armed Forces to sustain themselves, operate effectively with partners, and resist external pressures. This is the essence of projecting stability: not only deterring threats but enabling partners to govern their own security in a way that aligns with democratic principles and international norms.

[105] PfP Consortium, DEEP Handbook, op. cit.
[106] NATO 2016, NATO Policy on Countering Improvised Explosive Devices (C-IED), NATO Standardization Office.
[107] Kaim, M., & Kempin, R. (2019). NATO's Future in Crisis Management: Lessons from Iraq and Libya. Berlin: German Institute for International and Security Affairs (SWP).

3.6 NMI Advisory Effort

Advisory work lies at the heart of NMI. Effectiveness requires continuity, cultural awareness, and balance between reform and Iraqi ownership.[108] Advisors must navigate Iraq's highly centralized decision-making structure, where ultimate authority rests with the Chief of Defence and the Secretary-General of the Council of Ministers. Progress is achieved primarily through committees, where preparatory work is done before decisions are endorsed at higher levels.

The BI initiative illustrates advisory complexity. Strengthening transparency and accountability in Iraq's defence sector requires persistent engagement, cultural sensitivity, and in-person interaction to build trust. Advisors must carefully balance pushing reforms with respecting Iraqi ownership.

Coordination with bilateral initiatives - such as Canadian and Italian capacity building - ensures complementarity rather than duplication. [109] Advisors thus function as both technical experts and diplomatic intermediaries.[110]

Advisory success also depends on personal qualities: integrity, cultural sensitivity, and persistence. For instance, NATO's repeated efforts eventually led to Iraq's adoption of a gender strategy within its armed forces.[111]

---

[108] Schnaubelt, C. (2017). 'NATO's Role in Security Force Assistance: Strategic Utility and Operational Challenges.' NATO Defense College Research Paper No. 136.
[109] NATO 2021, NATO and Partner Contributions in Iraq.
[110] Collins, J. (2019). 'Advisors as Diplomats: The Human Dimension of Security Force Assistance.' Small Wars Journal.
[111] NATO 2020, Women, Peace and Security: NATO's Implementation of UNSCR 1325.

Effective advisors must cultivate professional bonds without crossing into personal dependency. They must apply emotional intelligence, maintain integrity, and avoid becoming overly sympathetic to their counterparts. Advisors are selected carefully, often requiring approval from NATO HQ, NMI leadership, and Iraqi authorities. Civilian advisors must adapt to Iraq's tribal, sectarian, religious and bureaucratic dynamics, which pervade the military environment and differ markedly from Western models.

Persistent education is key: NATO advisors must continuously filter in reform ideas, even when initial uptake is low. For example, repeated advisory engagement on integrating gender perspectives into Iraqi military education eventually led to the adoption of a gender strategy—something that was initially resisted. This persistence highlights how advisory work supports long-term structural reform despite initial resistance.[112]

3.7 Conclusions

SFA in the land domain is a cornerstone of NATO's contribution to MDO. By empowering partners to secure their own territory and institutions [113], NATO establishes the land domain as the anchor for multi-domain synchronization. Through NMI, NATO has demonstrated that capacity-building missions deliver strategic effects: reinforcing Iraqi sovereignty, reducing adversarial influence, and stabilizing NATO's southern neighbourhood.[114]

[112] Jackson, P. (2020). Capacity Building in Fragile States. London: Routledge.
[113] Gaub, op. cit.
[114] NATO 2022, Strategic Concept 2022, op. cit.

NMI illustrates how SFA can act as a force multiplier in MDO. By institutionalising reforms in logistics, doctrine, and education, NATO multiplies the effectiveness of other domains by grounding them in resilient land forces.[115] Ultimately, NMI represents NATO's shift from crisis response to crisis prevention, where partner self-sufficiency reinforces Alliance deterrence and defence in an interconnected operational environment [116]. It is no longer primarily NATO's boots on the ground, but those of partners strengthened through advice, training, and institution-building.

[115] Taylor, op. cit.
[116] Chuter, op. cit.

Chapter 4 — Maritime Domain

Of the five operational domains examined in this paper, the maritime domain presents the most complex institutional landscape for SFA. Land-based SFA has extensive doctrinal foundations in AJP-3.16 and AJP-3.2, supported by decades of operational experience from the Balkans to Afghanistan. Air and space SFA are emerging fields with identifiable institutional frameworks and growing Alliance investment. Maritime SFA, by contrast, remains the least codified dimension of the Alliance's assistance architecture: NATO doctrine acknowledges maritime security capacity building as one of its seven Maritime Security Operations tasks, but the mechanisms, sequencing, and institutional requirements through which SFA actually builds partner maritime capability in a multi-domain environment have not yet been systematically elaborated. This chapter does not resolve that gap. What it does — through the analytical work of the NATO Maritime Security Centre of Excellence (MARSEC COE) — is establish the operational and doctrinal foundation upon which a rigorous approach to maritime SFA in MDO will need to be constructed.

Understanding why that foundation is urgently needed requires stepping back from the purely military dimension of the maritime domain. Ninety per cent of global trade moves by sea. [117] *Ninety-five per cent of the world's cyberspace traffic travels through seabed communication cables.*[118]

[117] UNCTAD 2023, Review of Maritime Transport 2023, United Nations Conference on Trade and Development, Geneva.
[118] TeleGeography, Submarine Cable Almanac, 2023; see also NATO, Maritime Security: NATO's Role.

Offshore energy platforms supply a growing share of Europe's power generation, and port facilities anchor the logistical chains on which both civilian economies and military sustainment depend. The maritime domain is therefore not simply a space where naval forces manoeuvre — it is the connective tissue of the global economy, the substrate of digital communication, and a critical common on which state sovereignty, civilian prosperity, and military effectiveness simultaneously rely. The consequences of disrupting these commons have moved from theoretical to operational with striking speed. In September 2022, a series of underwater explosions severed three of the four pipes of the Nord Stream 1 and 2 gas pipelines in the Baltic Sea, in what Swedish and Danish investigators confirmed as deliberate sabotage.[119] *In October 2023, the Balticconnector gas pipeline between Finland and Estonia was damaged alongside two telecommunications cables in what Estonian and Finnish authorities concluded were related incidents caused by external mechanical force.*[120] *In November 2024, further submarine cable cuts in the Baltic Sea renewed concerns about a systematic campaign targeting undersea infrastructure in NATO's northern waters.*[121] *None of these incidents was countered in*

[119] Swedish Police Authority, preliminary investigation into the Nord Stream explosions, September 2022. Traces of explosives were subsequently confirmed: see Swedish Prosecutor's Office statement, October 2022. The sabotage of Nord Stream 1 and Nord Stream 2 occurred on 26 September 2022 in the Danish and Swedish economic zones of the Baltic Sea. German investigations remained ongoing as of 2025.

[120] Finnish National Bureau of Investigation (NBI), press conference statements, October 2023; Estonian Prime Minister Kaja Kallas, statement of 27 October 2023 confirming that the Balticconnector pipeline damage and the two telecommunications cable incidents were assessed as related. Finnish investigators identified the Hong Kong-flagged vessel Newnew Polar Bear as the probable cause.

[121] Multiple submarine cable incidents occurred in the Baltic Sea in November 2024, including damage to the C-Lion1 cable connecting Finland and Germany and cables

time. None resulted in attribution leading to accountability. Each exposed, in operational terms, the gap between the threat environment that NATO faces and the maritime security capabilities - above all, the partner maritime capabilities - that exist to respond to it.

The complexity of maritime SFA begins with the question of who the partner is. Unlike land operations, where SFA is typically directed at a national army operating within defined sovereign territory, maritime security involves a fundamentally more diffuse ecosystem of actors. National navies are only one element. Coast guards, maritime law enforcement agencies, port authorities, customs services, offshore energy infrastructure managers, private shipping operators, and subsea cable maintenance companies all play roles in maritime security that no single institution commands and no single doctrine currently integrates. The Gulf of Guinea illustrates this with particular clarity. A region where piracy, trafficking, illegal fishing, and organised crime intersect across the sovereign maritime spaces of more than twenty coastal states, the Gulf of Guinea has become the most active laboratory for multilateral maritime SFA currently operating. The Yaoundé Architecture, established in 2013 under UN auspices,[122] *the EU's Coordinated Maritime Presences initiative,* [123] *the European Peace Facility assistance measure of November*

linking Sweden and Lithuania. NATO and EU member states convened emergency consultations on critical undersea infrastructure protection.

[122] United Nations Security Council, Resolution 2018 (2011) and Resolution 2039 (2012) on acts of piracy and armed robbery at sea; Heads of State and Government of the Economic Community of Central African States (ECCAS) and the Economic Community of West African States (ECOWAS), Yaoundé Summit Declaration, June 2013.

[123] Council of the European Union, Coordinated Maritime Presences in the Gulf of Guinea, Council Decision (CFSP) 2021/103, 25 January 2021.

2023 supporting the navies of Ghana and Cameroon,[124] *and the long-running Africa Partnership Station programme — through which the United States Navy has conducted sustained maritime capacity building in West and Central Africa since 2007*[125] *— collectively represent the most developed existing model of maritime SFA. Yet even in this relatively resource-intensive environment, the results highlight structural limitations: partner navies remain dependent on external presence, interagency coordination between military and civilian maritime actors is inconsistent, and the transition from externally supported operations to nationally led maritime security remains elusive. The gap between where partner maritime forces are and where they need to be is, in a direct sense, the maritime SFA problem.*

Building partner capacity in this environment means not only training naval personnel but reforming the governance frameworks, interoperability standards, legal authorities, and interagency coordination mechanisms that allow these disparate actors to function as a coherent whole under pressure. This is precisely the kind of institutional reform work — deep, patient, and governance-focused — that distinguishes SFA in an MDO context from tactical training, and that this paper's central argument identifies as the necessary evolution of the Alliance's assistance approach.

---

[124] Council of the European Union 2023, European Peace Facility: Assistance measure in support of military actors and navies of Gulf of Guinea coastal states, €21 million, adopted 27 November 2023.

[125] U.S. Naval Forces Africa, Africa Partnership Station Programme, established 2007. See also: Jacobsen, J.K. and Nordby, J.R. (2015). Maritime Security in the Gulf of Guinea. Lettera: Royal Danish Defence College.

The MARSEC COE contribution examines this environment through the lens of NATO's seven Maritime Security Operations tasks, and the analysis maps directly onto what a mature maritime SFA programme would need to address. Supporting Maritime Situational Awareness (MSA) — the first and most foundational of these tasks — illustrates the point clearly. Effective MSA in the MDO era requires the fusion of space-based Intelligence, Surveillance, and Reconnaissance (ISR) assets including synthetic aperture radar and radio-frequency (RF) sensors with cyber-enabled data networks, electromagnetic spectrum monitoring, acoustic intelligence, and open-source information including Automatic Identification System (AIS) data. The exploitation of AIS has itself become a hybrid threat vector: state and non-state actors routinely manipulate vessel transponder data to conceal illicit transfers, sanctions evasion, and pre-positioning activity, with Russia's so-called shadow fleet — hundreds of tankers operating with falsified or disabled AIS signals to circumvent sanctions — providing the most operationally significant recent example.[126] *Partner maritime forces that lack the training to detect these manipulations, the network architecture to fuse multi-source intelligence, or the doctrinal frameworks to act on it are not simply less capable — they are structurally unable to contribute to the Recognised Maritime Picture that NATO-led operations depend on. Closing that gap is an SFA task, and*

[126] Windward AI, Russia's Shadow Fleet: How Deceptive Shipping Practices Enable Sanctions Evasion, 2023; United States Department of State, Guidance on the "Shadow Fleet" and Sanctions Evasion Schemes, 2024. AIS manipulation has been documented by multiple maritime intelligence providers including Lloyd's List Intelligence and Marine Traffic Analytics.

it operates simultaneously across the maritime, cyber, space, and information domains.

The same logic applies to critical infrastructure protection, which the MARSEC COE identifies as among the most pressing challenges in the contemporary maritime environment. The incidents described above — Nord Stream, Balticconnector, C-Lion1 — demonstrate that energy pipelines and subsea data cables cannot be secured through physical patrols alone. Their protection demands coordinated action across multiple domains: persistent space-based surveillance to detect anomalous vessel behaviour, rapid cyber-forensic capabilities to identify intrusions into port management and vessel traffic systems, electromagnetic countermeasures against GPS spoofing — a phenomenon extensively documented in the Baltic Sea and Black Sea, where commercial vessels have reported false position data consistent with deliberate electronic warfare activity[127] *- and legal attribution mechanisms that allow states to respond to hostile acts that deliberately remain below the threshold of armed conflict. Each of these capabilities requires not only technical investment but institutional structures that most partner maritime forces currently lack.*

The challenge of hybrid threats and freedom of navigation, examined in depth by the MARSEC COE, underscores how the maritime domain has become a preferred arena for grey-zone competition. The Houthi campaign

[127] Norwegian Centre for Research, Safety and Security (NORSAR) and maritime authorities in Finland, Estonia, and the Baltic states have documented systematic GPS/GNSS spoofing incidents in the Baltic Sea and Black Sea.

against commercial shipping in the Red Sea, which began in November 2023 and within months had disrupted a significant portion of global container traffic through one of the world's most critical strategic waterways, demonstrated the vulnerability of freedom of navigation to actors willing to employ anti-ship missiles, drone boats, and UUVs in combination.[128] *The EU's response — Operation EUNAVFOR Aspides, launched in February 2024 as a defensive maritime escort mission — required rapid integration of naval assets from multiple member states in a contested environment characterised by simultaneous kinetic and electronic threats.*[129] *The partner nations whose maritime forces NATO SFA programmes are designed to strengthen were largely absent from this response — not because of political unwillingness but because of institutional and capability gaps that no short-term assistance programme could bridge. This is the operational consequence of the maritime SFA deficit.*

The contribution's treatment of kill chains, resilient command and control, and unmanned system integration points toward the technical dimension of that same problem. Ukraine's use of maritime surface drones — autonomous and semi-autonomous naval USVs that conducted multiple

[128] IMF, Container Shipping Disruptions and the Red Sea Crisis, IMF Note, January 2024; UNCTAD, Impact of the Red Sea Crisis on Shipping and Trade, February 2024. Houthi attacks on commercial shipping began in October-November 2023 using anti-ship missiles, UAVs, and maritime drone boats.

[129] Council of the European Union, EUNAVFOR Aspides, Council Decision (CFSP) 2024/583, February 2024. The mission was mandated to protect freedom of navigation in the Red Sea, Gulf of Aden, and Indian Ocean.

strikes on Russian Black Sea Fleet assets between 2022 and 2024[130] *- provided the most operationally significant demonstration to date of how unmanned maritime systems can generate asymmetric effects in a contested naval environment. The doctrinal and procedural lessons from these operations are already influencing NATO's concept development work on unmanned maritime systems integration, precisely the kind of cross-domain, cross-actor innovation that the MARSEC COE's framework addresses. For partner maritime forces, absorbing these lessons requires not only platform investment but the training, procedural standardisation, and command frameworks that make unmanned system integration operationally reliable.*

The doctrinal and training dimensions analysed by MARSEC COE — concept development, exercise design, and the translation of lessons learned into standardised procedures — identify the specific entry points where SFA practitioners can most effectively engage. Experience from Operation EUNAVFOR Atalanta, the counter-piracy mission off the Horn of Africa that has included a maritime capacity-building component since its inception in 2008,[131] *reinforces this point: the most durable improvements in partner maritime capability in that theatre came not from*

[130] Ukrainian maritime surface drone (USV) operations against Russian Black Sea Fleet assets are extensively documented from 2022 to 2024, including attacks on the cruiser Moskva (in which Neptune anti-ship missiles were the primary weapon but ISR USVs played a role in targeting), the Kerch Bridge, and Russian naval bases at Sevastopol.

[131] Council of the European Union, Operation Atalanta (EUNAVFOR Somalia), established December 2008. The mission's capacity-building component — the Critical Maritime Routes Programme and direct mentoring of Somali and East African coast guards, represents one of the most sustained instances of maritime SFA in the Alliance's experience.

equipment transfers but from sustained advisory engagement in maritime law enforcement procedures, interagency coordination mechanisms, and the institutional frameworks that give partner coast guards and navies the authority and the procedures to act. Training personnel to exploit space-based ISR data, embedding cyber and information injects into maritime exercises, developing legal and attribution frameworks that commanders can apply with confidence, and codifying the employment of unmanned systems within maritime security tasks: these are the specific forms of institutional capacity that a maritime SFA programme grounded in MDO principles would need to deliver.

Read in this light, the MARSEC COE's contribution is not a detour from this paper's central argument — it is the maritime domain's operational evidence base for it. Every capability gaps the chapter identifies, every cross-domain integration challenge it describes, and every doctrinal recommendation it advances maps onto institutional deficits that SFA must address. The chapter does not design the maritime SFA programme; but it does is make that programme's necessity unmistakable and defines with precision the standard against which partner maritime forces, and the assistance efforts that support them, will ultimately need to be measured.

MDO in the Maritime Security Context

Capt. Levent Bahadir (OF-5) (TUR-N), Author

NATO Maritime Security Centre of Excellence (NATO MARSEC COE),

WMD Staff Officer & Acting Head, Concept and Doctrine Branch

4.1 Introduction

The maritime domain has long been central to NATO's deterrence and defence posture due to its function as both a space to manoeuvre and a platform for multi-sensor, multi-effects operations.[132] Through MDO, naval forces integrate surface combatants, submarines, unmanned maritime systems (UMS), maritime patrol aircraft, and helicopters with space-enabled communications, cyber-resilient networks, and Strategic Communications capabilities. This integration transforms the maritime battlespace into a multi-domain operational hub where ISR inputs from air and space converge with maritime operations to produce a Recognised Maritime Picture (RMP) that enhances MSA.

The employment of space-based ISR - including synthetic aperture radar (SAR), optical/infra-red, RF, and thermal sensors - extends situational awareness and enables decision-makers to respond faster and more effectively.[133] Similarly, integration with the cyber and information domains provides resilience against cyber intrusions, electronic warfare, and disinformation campaigns. In recent exercises, simulated cyberattacks, viral video disinformation, and narrative manipulation have underscored

[132] NATO 2011, Alliance Maritime Strategy, Brussels: North Atlantic Treaty Organization.

[133] NATO 2022, NATO Space Policy, Brussels: North Atlantic Treaty Organization.

the role of the cognitive domain in MDO, where controlling the information environment directly affects operational outcomes.

Practical demonstrations of MDO principles in maritime security exercises highlight the value of cross-domain cooperation. Scenarios built on real-world geographic contexts, such as the Gulf of Guinea, have tested abilities to address overlapping maritime security challenges through cooperative frameworks designed for "plug-and-play" interoperability.

In these environments, offshore patrol vessels, frigates, and UMS were supported by maritime patrol aircraft and helicopters, extending ISR reach and enhancing the effectiveness of maritime task groups. The incorporation of land-based considerations - such as the protection of critical infrastructure, port security, and the management of threats originating ashore - further demonstrated that maritime security cannot be isolated from the broader operational environment.

Command and control arrangements reflected the essence of MDO: synchronization of vertical and horizontal information flows, joint planning across domains, and alignment between NATO and non-NATO actors. This convergence validated that integrated ISR - fusing maritime, air, and space contributions - supports faster decision-making and improves the overall efficiency of operations.

The evolving character of threats in the maritime domain demands an MDO approach. Hybrid actors increasingly target subsea cables, offshore energy infrastructure, and ports, while also employing cyber tools, disinformation, and GPS spoofing to disrupt maritime stability.[134] The

[134] NATO 2023, Multi-Domain Operations in NATO – Explained, NATO Allied Command Transformation.

proliferation of UMS used by both state and non-state actors further complicates attribution, escalation management, and defence, raising both operational and legal dilemmas. These challenges require to employ MDO to be employed in support of its seven maritime security tasks: maintaining MSA; upholding Freedom of Navigation (FoN); conducting Maritime Interdiction Operations, countering proliferation of weapons of mass destruction, protecting Critical infrastructure (CI), supporting Maritime Counterterrorism (MCT), and contributing to maritime security capacity building.[135] [136]

From a multi-domain perspective, several key lessons emerge. Training personnel in the exploitation of space-based ISR data remains essential to harness the advantages of the space domain. Handover and takeover procedures between cross-domain units may be standardized to ensure interoperability. Strategic communications have proven decisive, functioning both as deterrence tools and as mechanisms for securing public and stakeholder support. Adaptable cooperative frameworks that can integrate diverse domain capabilities without heavy institutionalization have also demonstrated their value.

In operational terms, MDO transforms maritime security tasks by enabling rapid cross-domain cueing, layered critical infrastructure defence, and synchronized responses to hybrid threats. This requires effects-based planning, resilient command-and-control (C2) structures for contested environments, and the integration of legal expertise into operational planning from the outset.

[135] NATO, Alliance Maritime Strategy, op. cit.
[136] NATO, MDO in NATO – Explained, op. cit.

Ultimately, MDO provides the means to act cohesively, adapt rapidly, and operate resiliently in contested maritime environments. The decisive edge will belong to those who integrate capabilities faster, synchronize activities across domains, and maintain the resilience necessary to preserve the security, openness, and stability of the maritime commons.

4.2 Cross-Domain Coherence as a Strategic Imperative

NATO's deterrence and defence posture increasingly depends on the ability to achieve cross-domain coherence in both planning and execution. Contemporary adversaries operate seamlessly below, at, and above the threshold of armed conflict, employing a sophisticated mix of grey-zone tactics, lawfare, disinformation, cyber intrusions, electronic jamming, and rapid military posturing to erode the tempo of Allied cohesion and decision-making tempo.[137] Within the maritime sphere, these challenges are particularly evident in sustained pressures on strategic chokepoints, sea lines of communication (SLOCs), and critical maritime terrain. Adversaries simultaneously mount cyber and physical threats against CI—including ports, offshore energy platforms, and subsea cables—while proliferating unmanned systems and long-range precision fires that complicate access, manoeuvres, and escalation management. Against this backdrop, MDO evolve from being a force multiplier to a strategic imperative for maritime security in an increasingly contested environment.

[137] NATO 2021, NATO Warfighting Capstone Concept (NWCC), Brussels: North Atlantic Treaty Organization.

Sea control, a foundational objective of naval warfare, has always been multi-domain in nature. Traditionally achieved through the interaction of subsurface, surface, and air capabilities, it now exists as a highly data-centric and time-sensitive contest. The integration of space-based ISR, offensive and defensive cyber effects, and influence operations in the information domain transforms sea control into a layered competition where superiority depends less on platform-centric strength and more on the speed, precision, and resilience of cross-domain synchronization.[138] This shift fundamentally alters operational planning, requiring maritime forces to operate within a seamlessly connected network rather than as isolated units.

The defence of critical maritime infrastructure requires a fusion of military and civilian capabilities spanning all domains. Ports, offshore energy facilities, and subsea communication networks cannot be secured solely through physical measures. Instead, protection demands an integrated approach: rapid cyber-forensics, electromagnetic countermeasures, and legal-attribution mechanisms may complement patrols, interdiction operations, and maritime policing. NATO's approach, as outlined in its maritime security strategy, emphasizes institutionalized cross-sector integration to ensure that military operators, law enforcement agencies, private stakeholders, and Allied partners respond as a coherent whole to both immediate incidents and sustained hybrid campaigns.[139]

Effective deterrence at sea increasingly hinges on detection and attribution. Persistent multi-domain sensing - linking anomalies in the AIS with RF

[138] NATO, Alliance Maritime Strategy, op. cit.
[139] NATO, MDO in NATO – Explained, op. cit.

intercepts, SAR imagery, acoustic signatures, and open-source intelligence - allows elevation of both the political and operational costs of malign activities. Timely, credible, and publicly supportable attribution enhances deterrence across the multi-domain environment by degrading adversaries' ability to exploit ambiguity, thereby limiting their freedom of manoeuvre and constraining coordinated effects across domains.[140]

Resilience under disruption has emerged as a decisive factor in sustaining operational effectiveness. Adversaries are expected to target Global Navigation Satellite System (GNSS), Satellite Communication (SATCOM), and command-and-control nodes during crises. MDO compels operations to be designed contested and degraded environments, employing alternative positioning, navigation, and timing (PNT) solutions, issuing mission-type orders that empower subordinate initiative, and developing distributed kill chains capable of rerouting both decision authority and sensor-to-shooter links. This resilience is not static but may be continuously exercised, tested, and adapted to evolving threats.[141]

The rapid proliferation of unmanned and autonomous systems (UxS) presents both opportunities and challenges. Their persistence and reduced risk profile can be fully realised only when their tasking is coordinated across domains. This includes scenarios in which unmanned surface vessels (USVs) cue maritime patrol aircraft, unmanned underwater vehicles (UUVs) map seabed risks for subsea cable defence, and cyber capabilities secure sensor networks to ensure data integrity. UxS integration is not an isolated technological development but a core enabler

[140] NATO, NATO Space Policy, op. cit.
[141] NATO, NWCC, op. cit.

of MDO, demanding standardization of control protocols, data formats, and operational concepts across the Alliance.[142]

For NATO's seven Maritime Security Operations (MSO) task areas - supporting MSA, upholding FoN, conducting Maritime Interdiction Operations (MIO), countering the Proliferation of WMD, protecting CI, supporting Maritime Counterterrorism (MCT), and contributing to capacity building - MDO provides the connective tissue. It ensures that situational awareness is developed as a joint and interagency product; that interdiction and presence operations are supported by cyber and information measures to shape adversary behaviour; and that infrastructure protection fuses patrols with cyber-hardening, electromagnetic shielding, and legal instruments for attribution.[143]

The strategic imperative of MDO in the maritime domain lies not only in integrating capabilities across domains but also in transforming maritime security from discrete tasks into a continuous, adaptive, and resilient campaign. Embedding cross-domain sensing, decision-making, and effects delivery into every phase of MSOs ensures rapid, precise, and coordinated responses to evolving threats. This approach advances deterrence credibility, enhances resilience, and secures the maritime commons in line with the Alliance's long-term strategic vision.

[142] NATO, MDO in NATO – Explained, op. cit.
[143] NATO, Alliance Maritime Strategy, op. cit.

4.3 Hybrid Threats and Freedom of Navigation in MDO

The maritime domain, once defined primarily by conventional naval engagements, has transformed into a highly contested and interconnected battlespace situated at the crossroads of multiple, overlapping threat vectors. Adversaries now operate with increasing sophistication in the grey-zone, deliberately exploiting the seams between peace and armed conflict to achieve strategic effects while avoiding direct confrontation.[144] Hybrid threats have become a defining feature of this environment, as state and non-state actors combine covert and overt means to undermine established maritime norms. Illustrative cases include the clandestine deployment of UUVs near subsea communication cables, cyber intrusions into port management and vessel traffic systems, and the use of "dark" merchant shipping to conduct illicit transfers or evade sanctions. These activities blur the boundaries between military, economic, and informational conflict, demanding an integrated response that exceeds the capacity of traditional, single-domain naval operations.

Critical maritime infrastructure has emerged as both a high-value asset and a high-risk vulnerability. Offshore energy platforms, subsea data cables, port facilities, and associated logistics hubs not only underpin the global maritime economy but also sustain the operational posture. These assets are increasingly exposed to a spectrum of kinetic and non-kinetic threats ranging from sabotage and missile strikes to cyberattacks and

[144] NATO, NWCC, op. cit.

electromagnetic interference.[145] Defending them requires a layered, multi-domain approach that integrates maritime patrols with persistent space-based surveillance, rapid cyber-forensic capabilities, electromagnetic spectrum defence, and legal attribution mechanisms. Such a cross-domain framework ensures that operational decision-making is supported by accurate situational awareness and that strategic communication is reinforced through credible, verifiable responses.

FoN is a cornerstone of the international maritime order, is now contested through unconventional tactics. Adversaries employ disinformation campaigns to erode legitimacy, selectively enforce maritime claims to impose de facto control, and disrupt navigation confidence through GPS spoofing and jamming. These activities remain deliberately calibrated below the threshold of armed conflict, yet they steadily reshape the maritime strategic environment to the detriment of Allied interests.[146] Responding effectively requires the integration of information operations, electronic warfare, and legal countermeasures into maritime security posture: precisely the type of cross-domain orchestration that MDO provides.

The rapid proliferation of UMS, including USVS and UUVs, further complicates the operational calculus. These systems extend surveillance reach, enhance strike options, and reduce risks to personnel; yet their accessibility also provides adversaries with asymmetric means to challenge Allied presence, manoeuvrability, and escalation management. Hostile or unregulated use of UMS can saturate surveillance networks, conduct covert

[145] NATO, MDO in NATO – Explained, op. cit.
[146] NATO, Alliance Maritime Strategy, op. cit.

reconnaissance, or deliver disruptive payloads against CI.[147] The response may therefore extend beyond counter-platform measures to encompass multi-domain integration of detection, tracking, interdiction, and post-incident attribution capabilities.

MDO offers the doctrinal and technical foundation to confront these challenges. By ensuring that MSA is not confined to shipboard sensors or AIS data, but instead enriched by satellite imagery, cyber intelligence, electromagnetic spectrum monitoring, acoustic signatures, and open-source inputs, MDO transforms maritime security into a comprehensive cross-domain enterprise.[148] This integration enables rapid cueing of naval forces through dispersed sensor networks, synchronized application of kinetic and non-kinetic effects, and resilience in contested or degraded conditions.

Embedding MDO into maritime security is not a discretionary enhancement but an operational prerequisite for credible deterrence and effective defence. In an era where adversaries deliberately exploit the seams between domains, MDO closes those gaps by unifying sensing, decision-making, and action across the Alliance's full spectrum of capabilities. This integrated approach ensures that the maritime commons remain secure, open, and stable, and can maintain operational superiority in the face of increasingly complex and adaptive threats.

[147] NATO, MDO in NATO – Explained, op. cit.
[148] NATO, NATO Space Policy, op. cit.

4.4 Doctrinal and Training Dimensions of Maritime MDO

MDO provides a practical and adaptable framework to deter, and if necessary, defeat both hybrid and conventional threats targeting the maritime domain. By emphasizing integration, tempo, and resilience - and by systematically converting lessons from conferences, operations, and operator experience into standardized doctrine - MDO facilitates the Alliance's transition from multi-domain awareness to full multi-domain proficiency.[149] This transformation carries direct strategic consequences: a safer, more resilient maritime commons where freedom of navigation is preserved, CI is protected, and adversaries face fewer exploitable seams across domains.

Within the scope of Concept Development and Experimentation (CD&E), the efforts are directed toward aligning doctrine, tactics, techniques, and procedures (TTPs) by linking MSO tasks to specific MDO effects and identifying the cross-domain interdependencies that influence operational effectiveness. This includes clarifying the cyber preconditions and identifying the space-based indicators that are most effective for cueing patrols in CI protection.

NATO experimentation also includes the design of distributed kill chains and cue-target-effect playbooks linking maritime sensors, space and air ISR assets, cyber discovery tools, and information operations. These prototypes are validated through table-top exercises and controlled trials that increasingly incorporate unmanned systems. Furthermore, resilient

[149] NATO, NWCC, op. cit.

command-and-control (C2) patterns are developed for contested environments under the C2D2E (Command and Control in a Degraded, Denied, and Disrupted Environment) framework. Mission command, data minimization strategies, and alternative PNT solutions ensure continuity of operations when SATCOM or GNSS is compromised.[150]

Through Education, Training, and Exercises (ET&E), NATO ensures that its maritime forces are prepared to implement MDO effectively. This includes developing curricula that train watchstanders and analysts to integrate multi-intelligence inputs - such as RF geolocation, SAR change detection, acoustic UUV tracks, and open-source intelligence - into actionable products for commanders. Exercise design has also evolved, embedding cyber and information injects, CI attack simulations, and legal attribution dilemmas into scenarios. These injects ensure that learning objectives focus on synchronization and decision-making under complex, contested conditions rather than on platform-specific proficiency alone.[151]

In addition, NATO has codified the safe, lawful, and tactically effective employment of unmanned systems - USVs, UUVs, and UAVs - within MSO contexts, emphasizing their integration into joint ISR operations and their coordinated hand-off to naval, air, and space assets.

As a knowledge and policy integration platform, NATO systematically translates outputs from maritime security exercises, workshops, and conferences into doctrinal notes, standardization proposals, and training packages. Best practices include defending subsea cables, countering unmanned aerial and surface threats, and embedding information

[150] NATO, NATO Space Policy, op. cit.
[151] NATO, MDO in NATO – Explained, op. cit.

operations at sea. Interagency and industry linkages are also strengthened by convening military operators, coast guards, port authorities, energy companies, and technology providers to align technical standards—such as data APIs and sensor metadata—and refine hybrid threat response playbooks.

Legal and ethical framing is another essential component. NATO has increasingly emphasized the need to provide commanders with clear guidance on Rules of Engagement (ROEs), authorities, and proportionality in the employment of cyber and information capabilities across peacetime, crisis, and conflict scenarios.[152] [153]

Several key messages emerge from NATO's evolving MDO perspective in the maritime domain:

- MDO is no longer optional: hybrid threats are already exploiting cross-domain seams.
- Data discipline and interoperability are decisive enablers: without standardized protocols, multi-domain effects are delayed, and platform upgrades underperform.
- Exercises may test synchronization and resilience in C2: the true measure of success is the ability to deliver timely, coordinated effects under contested conditions, not merely platform-level excellence.

[152] NATO, Alliance Maritime Strategy, op. cit.
[153] NATO, MDO in NATO – Explained, op. cit.

- Unmanned systems achieve maximum value when orchestrated through MDO, amplifying presence, reach, and persistence; when employed in isolation, their impact is diminished.
- Legal, policy, and attribution frameworks may evolve in parallel with operational realities, so that commanders can confidently and lawfully employ cross-domain capabilities in defence of the maritime commons.

4.5 Operationalizing MDO: MSA, CI Protection, and Interdiction

The integration of MDO into NATO's maritime security framework represents both a profound challenge and a transformative opportunity. It challenges legacy approaches that treated operational domains in isolation, requiring a cultural and doctrinal shift toward seamless cross-domain orchestration. At the same time, it offers the opportunity to deter, disrupt, and defeat increasingly complex threats with greater precision, adaptability, and speed.[154]

Traditional naval operations emphasized domain-specific expertise—surface, subsurface, and air. In the MDO context, however, the maritime domain cannot be understood separately from its intersections with space, cyber, and the information environment. The growing use of hybrid tactics - such as GPS spoofing, disinformation, cyber intrusions into vessel traffic systems, and covert deployments of UMS - underscores the need for integration across all domains. This doctrinal shift ensures that maritime

[154] NATO, NWCC, op. cit.

forces are not only proficient within their own domains, but also achieve true multi-domain fluency, where sensing, decision-making, and effects delivery are synchronized across the full spectrum of operations.[155] [156]

One of the central contributions of MDO to NATO's maritime posture is its ability to link the Alliance's seven MSO tasks to cross-domain effects. Supporting MSA is strengthened by space-based ISR, cyber-enabled data fusion, and open-source intelligence. Upholding FoN now requires information operations and legal instruments alongside patrols. Protecting CI demands coordinated surveillance from space, maritime patrol aircraft, and UUVs, fused with cyber defence and electromagnetic spectrum resilience. Countering WMD proliferation, supporting MCT, and contributing to capacity building are likewise enhanced by the integration of cyber, space, and informational effects into traditional naval operations.

MDO implementation in the maritime domain requires sustained dialogue between military operators, civilian authorities, industry, and academia. NATO's knowledge-development platforms, workshops, and conferences provide venues for aligning perspectives on emerging technologies, legal frameworks, and operational requirements. These exchanges have generated actionable insights into integrating unmanned systems, cyber defence mechanisms, space-based ISR, and electromagnetic spectrum monitoring, enabling coherent, Alliance-wide approaches.[157] Such forums move beyond theoretical debates to produce interoperable solutions that are both technologically viable and strategically relevant.

---

[155] NATO, Alliance Maritime Strategy, op. cit.
[156] NATO, MDO in NATO – Explained, op. cit.
[157] NATO, NATO Space Policy, op. cit.

Live and simulated exercises serve as the laboratories where cross-domain integration is tested and validated. Fusion of maritime, air, and space ISR feeds into an RMP, integration of cyber defence into port security and MSA workflows, and the joint employment of unmanned and manned assets all provide empirical evidence for refining doctrine and training. These activities illustrate the shift from platform-centric proficiency to the orchestration of distributed, multi-domain effects under contested and degraded conditions.[158]

The operational potential of MDO can only be fully realized within a framework that is legally sound and politically acceptable. NATO has emphasized the importance of maritime law, ROEs, attribution mechanisms, and proportionality in applying cross-domain effects. Embedding legal expertise into operational planning ensures that commanders can act with confidence, knowing their actions rest on clear legal authority and are aligned with Alliance policy objectives.[159] [160]

In this way, MDO in the maritime domain is not a passive adaptation but an active architectural effort by the Alliance. By embedding MDO thinking into maritime doctrine, shaping multinational exercises to reflect cross-domain realities, and fostering deeper cooperation among Allies and partners, NATO amplifies its ability to operate across domains with precision, legitimacy, and resilience. This dual role, as both a doctrinal innovator and an operational integrator, places MDO at the heart of

[158] NATO, NWCC, op. cit.
[159] NATO, Alliance Maritime Strategy, op. cit.
[160] NATO, MDO in NATO – Explained, op. cit.

NATO's effort to secure the maritime commons in an era defined by complexity, interconnectivity, and persistent competition.[161]

4.6 Kill Chains, Resilient C2, and Unmanned Integration

The approach to maritime security within the MDO framework requires concept development, doctrinal refinement, advanced training, and operational experimentation to converge in a coherent manner. This convergence acts as a force multiplier for the Alliance's MDO objectives, ensuring that maritime security activities are not only aligned with principles of integration and synchronization but are also tested, validated, and operationalized in realistic contexts.[162] A central component of NATO's maritime security architecture is MSA. NATO doctrine emphasizes the blending of traditional naval sensors with open-source maritime data, commercial tracking feeds, and space-based ISR systems. Lessons from recent multinational exercises confirm that maritime MSA is significantly enhanced when fused with cyber intelligence, electromagnetic spectrum monitoring, and air-domain reconnaissance assets. This cross-domain fusion produces actionable decision-support products, enabling commanders to make faster, more informed choices and anticipate adversary behaviour with greater accuracy. In effect, MDO transforms MSA from a static, platform-based picture into a dynamic, networked, and adaptive operational asset.[163]

[161] NATO, MDO in NATO – Explained, op. cit.
[162] NATO, NWCC, op. cit.
[163] NATO, Alliance Maritime Strategy, op. cit.

CI protection has emerged as a decisive aspect of maritime security. NATO's recent work on MCT and CI defence integrates lessons from real-world incidents with insights from complex exercises.[164] Protection of ports, offshore energy platforms, and subsea data and power cables demand not only physical patrols and surveillance but also synchronized cyber, space, and legal measures. Layered CI protection therefore involves naval forces, coast guards, private sector operators, and national authorities acting as a coordinated whole. Such a multi-domain, multi-actor approach ensures that vulnerabilities are reduced, resilience is strengthened, and protection efforts extend beyond the immediate area of operations into the cyber and informational domains.[165]

MIO have also evolved in the MDO context. Traditionally centred on boarding operations, vessel tracking, and inspection, MIO now requires integration of cyber, space, and information capabilities and activities into every phase. For example:

- Cyber reconnaissance can identify vulnerabilities in suspect vessels prior to boarding.
- Space-based ISR confirms vessel positioning and detects deviations from declared routes.
- Targeted information operations shape the behaviour of suspect vessels and their operators before military action is taken.

By embedding these cross-domain tools into MIO doctrine and training, NATO ensures that its maritime forces can respond to hybrid threats with agility, precision, and legal legitimacy.

[164] NATO, MDO in NATO – Explained, op. cit.
[165] NATO, NATO Space Policy, op. cit.

Taken together, these capabilities position MDO as an operational enabler rather than a theoretical construct. Embedding cross-domain integration into MSO enhances the ability to maintain maritime superiority, protect CI, and deter adversary actions in contested and complex environments. This transformation reflects a broader shift within the Alliance: from multi-domain awareness to multi-domain proficiency, where every maritime task is executed as part of an integrated, resilient, and adaptive campaign.[166]

4.7 Strategic Conclusions: Embedding MDO in Maritime Security

NATO plays a proactive role in shaping the operationalization of MDO principles in the maritime environment by combining targeted research, concept development, and experimentation. These initiatives are designed to transform MDO from a doctrinal aspiration into an operational reality, testing concepts, validating innovative tactics, and ensuring interoperability across domains in contested and complex environments.

One of the most significant areas of development within NATO's maritime MDO framework is the design of cross-domain kill chains. These operational playbooks connect maritime, air, space, and cyber sensors into integrated cue-target-effect sequences. The purpose is to deliver decisive effects within minutes rather than hours, thereby outpacing adversary decision-making cycles. For example, an anomaly detected by a USV during patrol could immediately trigger a request for high-resolution satellite imagery, which in turn cues airborne ISR or interdiction missions.

[166] NATO, NWCC, op. cit.

Such synchronized, multi-domain responses compress targeting cycles, increase operational success rates, and reduce the exposure of manned assets.[167]

MDO also requires resilient command-and-control (C2) systems that can withstand adversary interference. Recognizing that jamming, cyber intrusions, and satellite degradation will be employed to undermine NATO's C2 infrastructure, the Alliance is experimenting with alternative positioning, navigation, and timing (alt-PNT) solutions, decentralized command structures that empower subordinate initiative, and low-bandwidth, secure data exchange protocols. These approaches simulate disruption scenarios and ensure that NATO maritime forces remain operationally effective in degraded environments.[168]

Operational success in MDO depends not only on effectiveness but also on legitimacy. NATO increasingly embeds legal expertise directly into MDO concept testing to ensure that all multi-domain effects - particularly in the cyber and information environments - comply with the law of armed conflict, the United Nations Convention on the Law of the Sea (UNCLOS), and NATO's established ROEs.[169] This early integration prevents unintentional policy or legitimacy risks while providing commanders with confidence that their actions are both lawful and politically defensible.

A further dimension of experimentation lies in the integration of unmanned systems. NATO trials have explored how USVs and UUVs can be tasked alongside air and space ISR assets to achieve mission objectives. Examples

[167] NATO, MDO in NATO – Explained, op. cit.
[168] NATO, NATO Space Policy, op. cit.
[169] NATO, Alliance Maritime Strategy, op. cit.

include continuous CI surveillance with USVs, seabed mapping and subsea cable inspection with UUVs, and the employment of unmanned systems in mine countermeasure operations. Integrated tasking enhances persistence, extends operational coverage, and reduces risks to personnel and high-value manned assets.[170]

Through these CD&E activities, NATO ensures that maritime forces are equipped with validated, interoperable, and legally sound methods for applying MDO principles in real-world operations. By acting as a testbed for cross-domain innovation, the Alliance accelerates adaptation to emerging threats and projects a credible, integrated maritime security posture across the full spectrum of peace, crisis, and conflict.[171]

4.8 Toward a Secure and Resilient Maritime Commons

MDO is examined through the lens of NATO's evolving doctrine, the distinctive challenges of the maritime environment, and the mechanisms by which MDO principles are translated into operational reality. From the preceding discussion, several consistent themes emerge that collectively underscore the urgency and inevitability of adopting MDO as a foundational element of NATO's maritime security posture.

First, MDO is no longer optional in the maritime context; the complexity, speed, and cross-domain nature of modern threats demand integrated action as a baseline capability, not as a supplementary enhancement. Second, the maritime domain is inherently multi-domain in character;

[170] NATO, MDO in NATO – Explained, op. cit.
[171] NATO, NWCC, op. cit.

naval forces operate simultaneously in the surface, subsurface, air, space, cyber, and information environments, making them natural actors for cross-domain synergy.[172] Third, interoperability - legal, technical, and cultural - is as decisive as firepower itself; without standardized frameworks and shared practices, the potential of cross-domain operations is reduced to isolated tactical actions. Fourth, resilience is the cornerstone of credibility in MDO; maritime forces must be able to operate in contested, degraded, and denied environments, particularly within cyberspace and the electromagnetic spectrum.

The integration of MDO into maritime security represents both a strategic necessity and a competitive advantage. It is a necessity because adversaries already employ multi-domain methods, blending hybrid tactics with conventional capabilities to exploit seams in NATO's posture. Without a deliberate MDO framework, the Alliance risks responding in a fragmented manner to coordinated threats. It is an advantage because NATO's multinational composition, diverse capabilities and established command structures provide an unmatched foundation for generating synchronized cross-domain effects - provided that integration is pursued deliberately and systematically.[173]

The maritime domain amplifies both the risks and opportunities inherent to MDO. Its vast geography, complex legal regimes, and reliance on the global commons make it a preferred arena for adversary hybrid activity. At the same time, these very characteristics offer NATO an unmatched stage on which to demonstrate credible deterrence, rapid decision-making, and

[172] NATO, Alliance Maritime Strategy, op. cit.
[173] NATO, MDO in NATO – Explained, op. cit.

precise, coordinated action across multiple domains. The sea has always been a space of manoeuvre, commerce, and strategic contest. In the 21st century, it has become a fully-fledged cross-domain battlespace where the decisive edge will belong to those who can integrate capabilities faster, act more cohesively, and adapt with greater resilience than their opponents.[174] [175]

Ultimately, embedding MDO principles into the very fabric of maritime security - across doctrine, training, exercises, legal frameworks, and capability development - ensures that the Alliance safeguards the maritime commons, deters aggression, and projects stability on a global scale. The imperative is clear: deliberate action must be taken before adversaries transform operational seams into exploitable vulnerabilities. With such action, NATO can preserve the maritime domain as a secure, open, and stable global commons for decades to come, retaining the decisive edge in an era defined by speed, complexity, and persistent competition.

[174] NATO, NWCC, op. cit.
[175] NATO, MDO in NATO – Explained, op. cit.

Chapter 5 — Air Domain

Air-related SFA covers two fundamentally different activities: using airpower to support the delivery of SFA and helping a supported nation to develop its own air component. The shift to MDO does not substantially alter the second. Building a partner air force remains a long-term, institutionally focused endeavour governed by largely unchanged fundamentals. What MDO transforms first is how airpower is employed in support of SFA delivery in an environment where air effects are no longer self-contained but deeply interdependent with land, maritime, cyber, and space capabilities. This distinction, developed by the Joint Air Power Competence Centre (JAPCC) in the contribution that follows, is the analytical foundation on which this chapter rests.

That foundation connects directly to the paper's central argument. If SFA is to function as a structural enabler of MDO rather than a supplementary activity, it cannot approach the air domain through the lens of platform transfer or tactical training alone. It must understand air power as a cross-domain integrator - a capability that senses, connects, moves, and accelerates effects - and must design assistance around the operational outcomes that partner forces need to generate rather than the platforms or domain architectures through which those outcomes are traditionally delivered. The effects-based, domain-agnostic framework that the chapter proposes is precisely this shift in analytical register.

The practical implications are concrete. NMI, examined in Chapter 3, operates in an air environment shaped by A2/AD constraints, cyber vulnerabilities in command-and-control networks, and the proliferating

presence of unmanned systems that complicate airspace management at every operational level. Advisory work on defence planning in that context cannot treat air-enabled effects as a planning constant. It must account for the cross-domain dependencies — resilient data links, spectrum access, space-based navigation and timing — that determine whether those effects can be delivered safely and predictably and build the institutional conditions accordingly. This is the point at which air domain SFA becomes indistinguishable from the enterprise of broader institutional reform enterprise that MDO demands.

Understanding the Air Domain for Effective SFA Delivery in a Multi-Domain Context

Lt. Col. Gwendolyn Bakx (NLD-ASF), Author

Joint Air Power Competence Centre (JAPCC), Staff Officer Air Leadership & Transformation, C5ISR & Space Branch

5.1 Introduction

NATO's adoption of Multi-Domain Operations provides the strategic context for how the Alliance plans, organises, and employs its forces, including those in the Air Domain.[176] [177] Rather than restating the broader implications of MDO for NATO as a whole, this contribution focuses on what MDO means specifically for the Air Domain and how those implications shape the way SFA should be conceived and delivered. What is important to notice is that air-related SFA covers two areas: using airpower to support SFA delivery and helping the supported nation develop its air component.[178] The shift to MDO does not substantially affect the latter, as NATO does not impose MDO on supported nations and the fundamentals of building an air force remain largely unchanged. For that reason, this chapter concentrates on the former: how airpower contributes to SFA delivery in a multi-domain environment.

[176] NATO 2021, Warfighting Capstone Concept (NWCC) (NATO Allied Command Transformation ACT).
[177] NATO 2023, NATO Multi-Domain Operations (MDO) Concept.
[178] NATO 2025, Allied Joint Doctrine for Security Force Assistance (SFA) NATO AJP-3.16, Allied Joint Doctrine for Security Force Assistance, Edition B, Version 1.

The Air Domain remains central to NATO's deterrence and defence posture, providing rapid sensing, mobility, precision engagement, and command-and-control functions that underpin the Alliance's ability to understand, decide, and act.[179] At the same time, these functions are increasingly interdependent with capabilities from other domains.[180] [181] Advances in land-based fires, maritime strike, cyber effects, and space-enabled sensing mean that multiple domains now contribute to effects once considered the exclusive preserve of airpower. The growing use of unmanned and remotely-piloted systems further accelerates this shift, expanding the Air Domain's reach while deepening its reliance on resilient data links, electromagnetic spectrum access, and space-enabled services.

This evolution reframes the role of airpower. The Air Domain has become a cross-domain integrator and a critical node within a wider multi-domain network, valued for its ability to connect, synchronise, and accelerate effects across domains.[182] These integrative functions (from sensing and mobility to precision engagement and C2) form the basis of the Air Domain's contribution to MDO and will be explored in more detail in the following section. The implications for SFA are direct. SFA must be informed by the ways in which air capabilities interact with land, maritime, cyber, and space systems in contemporary operations. Depending on

[179] NATO 2026, Allied Joint Doctrine for Air and Space Operations (AJP-3.3, Edition C, Version 1) (NATO Standardization Office 2026).
[180] NATO Allied Joint Doctrine (AJP-01, Edition F, Version 1) op. cit.
[181] NATO 2023, NATO Multi-Domain Operations (MDO) op. cit.
[182] E.g. Deptula, The Combat Cloud: Envisioning Airpower in 21st Century Warfare (Mitchell Institute for Aerospace Studies 2014).

context, this may include aligning selected processes, standards, or frameworks where they enable interoperability and effectiveness. Ultimately, SFA must strengthen the ability of supported forces to integrate air-enabled effects into their broader activities, ensuring that SFA delivery remains coherent, resilient, and effective in a multi-domain environment.

5.2 The Air Domain in Modern Conflict

5.2.1 The Evolving Role of Airpower

Airpower remains indispensable to modern military operations, but the context in which it is employed has changed significantly. Rather than operating as a largely self-contained instrument, air forces now function within a dense web of cross-domain dependencies and complementary capabilities. Three trends illustrate this evolution.

Effects are now multi-domain by design[183]

Capabilities that were once the exclusive preserve of air forces are now distributed across multiple domains. Intelligence, surveillance, and reconnaissance (ISR) is no longer solely airborne; it is complemented by space-based sensors, cyber reconnaissance, and ground-based systems. Precision strike is similarly shared: long-range land fires, maritime strike platforms, and even cyber effects can deliver outcomes that previously required air assets. As a result, airpower is no longer the single point of entry for many critical operational effects. Instead, it is one contributor within a broader, interconnected system.

[183] NATO 2022, Allied Joint Doctrine (AJP-01), Edition F, Version 1; Joint Air Power Competence Centre, MDO white paper (forthcoming).

Airpower is increasingly interdependent with other domains[184]

Modern air operations rely on a dense web of cross-domain enablers. Space-based services provide navigation, timing, and communications. Cyber-secure networks underpin command and control, mission planning, and data dissemination. Access to the electromagnetic spectrum is essential for sensing, targeting, and survivability. These dependencies mean that airpower's effectiveness is directly tied to the resilience and availability of capabilities in the land, maritime, cyber, and space domains. Disruptions in any of these areas can degrade or even neutralise air operations.

Airpower's comparative advantage lies in integration[185]

In contemporary operations, airpower's unique value stems from its ability to link, synchronise, and accelerate activity across domains. While space-based capabilities enable the information architecture that supports these activities, air forces provide wide-area and directed sensing, rapid mobility, and airborne command-and-control that allow dispersed forces to coordinate and act coherently. Because these functions can be applied directly at the point of action and in real time, they enable forces across the domains to respond, manoeuvre, and collaborate at speed. This makes airpower a practical integrator of cross-domain activity. It is this integrative

[184] RAND 2022 Corporation, Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea.

[185] Deptula 2017, The Combat Cloud: Envisioning Airpower in 21st Century Warfare (Mitchell Institute for Aerospace Studies 2014); Joint Air Power Competence Centre, Air Warfare Communication in a Networked Environment: An Interdisciplinary Analysis.

role, rather than the contribution of any single platform or capability, that gives airpower its enduring relevance in modern conflict.

5.2.2 Threats and Challenges Affecting the Air Domain

Supported nations in SFA often operate in challenging environments in which a range of operational, technological, and institutional pressures shape how airpower can be employed to support SFA delivery. These challenges influence what air-enabled effects can be generated, how reliably they can be integrated with other domains, and what SFA practitioners must anticipate when planning or conducting activities in or alongside the Air Domain.

- **A2/AD systems limiting access and manoeuvre[186]**

  Layered A2/AD networks compress airspace and restrict freedom of manoeuvre, making even routine air operations risky for nations without robust counter-air or SEAD capabilities. This limits when and how airpower can support SFA activities and places a premium on survivability, dispersion, and cross-domain coordination.

- **Cyber and electromagnetic vulnerabilities across aircraft, networks, and C2[187]**

  Air operations depend on digital systems that are often insufficiently protected. Cyber intrusions can disrupt mission

[186] Joint Air Power Competence Centre, 2020, Challenged Air Superiority: Adapting to the Drone and Missile Age (JAPCC 2024); Justin Bronk, Russian and, particularly, Chinese capabilities now pose greater threats to Western air power than in 2020 (RUSI Institute 2026).
[187] Justin Bronk, Airborne Electromagnetic Warfare is Critical for NATO's Airpower Edge, (RUSI Institute 2024).

planning, corrupt data, or sever C2 links, undermining the reliability of air-enabled support to SFA and creating operational uncertainty.

- **Space-based disruptions to navigation, timing, and communications**[188]

  Airpower's reliance on satellite-enabled services makes it vulnerable to jamming, spoofing, and interference. For supported nations with limited redundancy, disruptions in the space domain can quickly degrade the availability and precision of air-enabled effects.

- **Proliferation of unmanned systems**[189]

  The growing density of unmanned systems, friendly and adversarial, creates congested and unpredictable airspace. Adversary drones complicate air defence and electromagnetic protection, affecting the safety and timing of air support to SFA activities.

- **Technological disparities limiting interoperability**[190]

  Legacy platforms and non-standardised data architectures can hinder integration between NATO air assets and supported forces.

[188] RAND, 2025, Lessons from the War in Ukraine for Space: Challenges and Opportunities for Future Conflicts, (RAND Corporation).
[189] Joint Air Power Competence Centre, 2021 A Comprehensive Approach to Countering Unmanned Aircraft Systems; Joint Air Power Competence Centre, Challenged Air Superiority: Adapting to the Drone and Missile Age (JAPCC 2024).
[190] Zajec, 2021, Integration and Interoperability for Multi-Domain Operations in the Coalition Environment: Challenges for European Air Combat Fleets.

These disparities reduce the speed and fidelity of information sharing and may limit the types of air-enabled support that can be employed safely.

- **Fragmented institutional structures**[191]
  Unclear authorities, weak governance, or fragmented sustainment processes can affect the predictability and continuity of air support to SFA. These institutional issues influence planning assumptions and the reliability of air-enabled effects.

- **Sustainment and lifecycle constraints**[192]
  Limited maintenance capacity, supply chains, and technical expertise can reduce aircraft availability and the persistence of air-enabled support. These constraints shape what airpower can provide during SFA activities and require realistic expectations about endurance.

Together, these challenges define the practical limits of what airpower can provide in support of SFA and what levels of integration into MDO are feasible. They also highlight where SFA must focus to ensure that air-enabled effects are credible, resilient, and usable in real operational

[191] NATO, 2024, Allied Joint Doctrine (AJP-3.3.5, Edition C, Version 1) (NATO Standardization Office); Joint Air Power Competence Centre, Integrating the Blue and Green Domains (JAPCC 2025).
[192] War on the Rocks, 2024, Turbulence Ahead: The Maintenance Workforce Dilemma Threatening the Future of Airpower, RAND, The Russian Air Force is Hollowing itself Out: Air Defences for Ukraine Would Speed that Up (RAND Corporation, 2024).

conditions. Without understanding these constraints, SFA risks assuming levels of air support that cannot be delivered or sustained.

5.2.3 Key Functions of the Air Domain in MDO

In multi-domain operations, the Air Domain contributes not by acting as a standalone provider of effects, but by enabling the integration, synchronisation, and acceleration of activity across domains. Air capabilities connect sensors to decision-makers, extend the reach of dispersed forces, and link manoeuvre to effects, thereby enhancing the coherence and tempo of joint operations. Four core functions underpin this integrative role and shape how airpower supports the delivery of SFA in complex environments.

Cross-domain sensing and intelligence fusion

Air platforms provide wide-area, rapidly taskable sensing that complements land, maritime, cyber, and space-based collection.[193] Their value lies in the ability to generate timely, multi-source understanding that supports decision-making and enables effects across domains. Airborne ISR can validate or cue other sensors, refine targeting, and enhance situational awareness for both NATO and supported forces, strengthening the information foundations of SFA activities.

Mobility, access, and resilience

Air mobility enables the rapid movement of personnel, equipment, and information across dispersed or contested terrain. Beyond transport, it

[193] Deptula 2014, The Combat Cloud: Envisioning Airpower in 21st Century Warfare (Mitchell Institute for Aerospace Studies).

provides operational access, sustains distributed forces, and offers alternatives when ground lines of communication are constrained. These attributes allow SFA teams and supported units to maintain tempo, reach otherwise inaccessible areas, and remain resilient in dynamic environments.

Precision engagement and fires integration

Airpower delivers precise, scalable, and time-sensitive effects that can be synchronised with fires from other domains.[194] Air-delivered fires shape the battlespace, create windows of manoeuvre, and reinforce land, maritime, cyber, or space-generated effects.[195] The contribution is not limited to strike; it includes the ability to integrate targeting, timing, and effects across domains in support of partner operations.

Command and control (C2)

Air-enabled C2, through airborne platforms, relay nodes, and communications architectures, provides flexible and survivable coordination across wide areas.[196] It helps maintain coherence among dispersed forces, bridges gaps when terrestrial networks are degraded, and supports the integration of effects across domains. For SFA, this enhances the supported nation's ability to plan, coordinate, and execute operations even in contested conditions.

---

[194] NATO 2022, Allied Joint Doctrine (AJP-01, Edition F, Version 1); NATO Allied Joint Doctrine for Air and Space Operations (AJP-3.3, Edition C, Version 1) (NATO Standardization Office 2026).

[195] NATO 2026 Allied Joint Doctrine for Air and Space Operations (AJP-3.3, Edition C, Version 1) (NATO Standardization Office 2026).

[196] Joint Air Power Competence Centre, 2017, Air Warfare Communication in a Networked Environment: An Interdisciplinary Analysis.

5.2.4 The Role of Unmanned Air Assets in Contemporary Operations

Unmanned and remotely-piloted air systems have become an increasingly prominent feature of modern conflict, offering persistence, survivability, and operational reach at lower cost and risk.[197] Their value lies not in replacing traditional airpower functions, but in extending them. At the same time, their effectiveness depends on resilient data links, electromagnetic spectrum access, and space-enabled services, making them highly sensitive to cyber and electronic warfare threats. For SFA delivery, unmanned systems can enhance situational awareness, mobility, and protection, but they also introduce new vulnerabilities that must be understood and mitigated.[198]

5.3 An Effects-Based, Domain-Agnostic Approach to SFA in an MDO Environment

Multi-Domain Operations require planners and practitioners to think in terms of the effects that must be generated across the competition–crisis–conflict spectrum, rather than the individual domains that produce them. Assistance is therefore structured around the effects supported nations need to generate (such as situational awareness, mobility, protection, or coordinated action) rather than the platforms or organisations that traditionally deliver them.

---

[197] IFRI 2025, Tourret, Design, Destroy, Dominate. The Mass Drone Warfare as a Potential Military Revolution Joint Air Power Competence Centre, A Comprehensive Approach to Countering Unmanned Aircraft Systems (JAPCC 2021).
[198] DIIS Policy Brief 2024, Clausen, Non-State Armed Groups in the Sky.

For SFA, this means shifting from platform-centric or domain-siloed approaches to a focus on operational outcomes. Domain expertise remains essential, but it must be applied in ways that strengthen the supported nation's ability to generate and integrate effects across domains. This helps ensure that SFA remains realistic and sustainable, avoiding solutions that exceed institutional capacity or create dependencies that cannot be maintained in contested environments.

5.3.1 What "Domain-Agnostic" Means in Practice

Assistance focuses on strengthening the supported nation's ability to generate and integrate effects in ways that are realistic and sustainable within its own context. This does not require the supported nation to adopt MDO as a formal concept for NATO to operate in an MDO environment, and many lack the resources, institutional maturity, or strategic incentives to pursue full multi-domain integration. What matters for SFA is understanding how multi-domain dependencies shape the operational environment and the delivery of assistance. This includes where air-enabled effects can add value, where they may be constrained, and how they interact with existing national capabilities and limitations. At the same time, a domain-agnostic approach does not reduce the importance of understanding the Air Domain or any other domain. Instead, it requires clarity about how each domain contributes to joint outcomes and how those contributions interact.

5.3.2 Why the Air Domain Matters in the Effects-Based Model

Airpower's value in MDO lies in its ability to sense, connect, move, and integrate effects across dispersed and contested environments. These

functions enhance the effectiveness of land, maritime, cyber, and space capabilities by improving situational awareness, accelerating decision-making, and enabling coordinated action.

For SFA, this means that airpower should be understood as a set of functions that can support the delivery of assistance and strengthen the supported nation's ability to operate within a multi-domain context.[199] Airborne sensing can improve situational awareness for partner forces conducting security operations. Air mobility can extend the reach of SFA teams and supported units, enabling them to operate in dispersed or inaccessible areas. Air-enabled C2 can enhance coordination across geographically separated elements. Precision engagement, whether kinetic or non-kinetic, can support partner manoeuvre or reinforce effects generated from other domains.

Taken together, these considerations form the conceptual foundation for understanding how airpower supports the delivery of SFA in contemporary operational environments. They provide the bridge between the characteristics of the Air Domain in MDO (Section 5.2) and the practical implications for SFA design and execution (Section 5.4), ensuring that assistance remains coherent, resilient, and aligned with the realities of modern conflict.

[199] NATO 2026 Allied Joint Doctrine for Air and Space Operations (AJP-3.3, Edition C, Version 1) (NATO Standardization Office).

5.4 Implications for SFA Delivery in an Air-Enabled MDO Context

In an MDO environment, SFA is about enabling effects, not delivering activities. This requires a shift from platform-centric assistance to strengthening the institutional, technical, and operational foundations that enable air-enabled effects in an MDO environment to support SFA activities. Three implications stand out.

5.4.1 SFA Must Prioritise Cross-Domain Enablers

Air-enabled SFA depends on enablers that sit across multiple domains: resilient data links, cyber-secure networks, spectrum access, and space-based services. These underpin the ability of air platforms to sense, communicate, navigate, and integrate effects. Without them, airpower cannot reliably support SFA activities, regardless of the platforms available or the intent to employ them.

For SFA practitioners, this means identifying where these enablers are fragile, absent, or contested, and tailoring assistance accordingly. It may involve supporting partners in establishing basic digital hygiene, improving electromagnetic spectrum management, or strengthening the resilience of command-and-control networks. The objective is not to build advanced air capabilities, but to ensure that the conditions exist for air-enabled effects to be delivered safely and predictably.

5.4.2 SFA Must Account for Institutional and Operational Realities

Airpower can enhance mobility, sensing, and protection for SFA teams and supported forces, but the ability to employ these functions safely depends on governance mechanisms, procedures, and coordination structures that many supported nations may not yet possess. Weak authorities, fragmented command arrangements, or inconsistent safety processes can limit the availability and reliability of air-enabled support.

SFA must therefore begin with a clear understanding of the supported nation's institutional maturity, operational culture, and risk thresholds. This includes assessing how airspace is managed, how missions are authorised, how information flows between units, and how safety is enforced. Where these foundations are underdeveloped, NATO can create or reinforce the necessary enabling environment to allow air-enabled effects to support SFA activities, while helping the partner build its own systems over time. The aim is to ensure that air-enabled effects are usable in the near term and sustainable in the long term.

5.4.3 SFA Must Promote Interoperability and Joint Integration

Air-enabled SFA requires alignment with joint planning, fires integration, and multinational command-and-control processes. Airpower rarely operates in isolation; its value lies in how it synchronises with effects generated from other domains. For SFA, this means understanding how air-enabled contributions fit into wider operational frameworks and ensuring they remain compatible with NATO procedures, even when supported nations are not yet able to integrate them independently.

Interoperability in this context is less about matching platforms and more about aligning processes, information flows, and decision-making cycles. Where these capacities are underdeveloped, NATO can provide or reinforce the necessary liaison structures, planning mechanisms, and coordination processes to enable air-enabled effects in the near term, while supporting the partner in building its own systems over time. The aim is to ensure that air-enabled contributions are coherent and usable today, and progressively more sustainable as national structures mature.

5.5 Recommendations

The implications outlined in Section 5.4 point to a set of practical steps that SFA practitioners, NATO, and supported nations can take to ensure that air-enabled effects contribute meaningfully to SFA delivery in an MDO environment. These recommendations focus on strengthening cross-domain enablers, improving institutional coherence, and ensuring that air-enabled contributions remain safe, predictable, and interoperable.

5.5.1 For SFA Practitioners

- **Adopt an effects-based, domain-agnostic approach to planning and delivery:** Practitioners should begin by identifying the effects required to support SFA activities and then determine which air-enabled functions can contribute to those outcomes.
- **Identify cross-domain dependencies early:** Air-enabled effects rely on cyber resilience, spectrum access, data links, and space-based services. Practitioners should assess these

dependencies at the outset and determine where NATO must temporarily provide or reinforce them.

- **Operate within safe, governed, and interoperable frameworks:** Where national structures are underdeveloped, practitioners should work with NATO elements to create or strengthen the enabling environment required for air-enabled effects to support SFA activities.
- **Tailor assistance to institutional and operational realities:** Effective SFA requires understanding what the supported nation can absorb and employ safely in the near term and adjusting expectations and methods accordingly.

5.5.2 For NATO

- **Provide clear guidance on integrating air-enabled effects into SFA:** NATO doctrine should articulate how airpower contributes to SFA delivery in an MDO environment, including cross-domain dependencies and enabling requirements.
- **Strengthen education and training on air-enabled SFA:** Courses, exercises, and wargames should expose practitioners to the opportunities and constraints of operating with air-enabled effects in contested, degraded, or denied environments.
- **Ensure the availability of scalable planning tools and frameworks:** These should help SFA planners identify relevant air-enabled functions, assess enabling requirements, and determine when NATO must temporarily provide integration mechanisms.

- **Support partners in developing resilience to air-related vulnerabilities:** This includes cyber resilience, electromagnetic spectrum management, and counter-UAS measures relevant to SFA operations.

5.5.3 For Supported Nations

- **Strengthen essential enablers that allow air-enabled effects to support SFA activities:** Priorities include secure communications, basic digital hygiene, spectrum management, and resilient C2 networks — all of which underpin safe and reliable air-enabled support.
- **Develop simple, coherent coordination mechanisms:** Even basic processes for airspace coordination, mission authorisation, and information sharing can significantly improve the safety and effectiveness of air-enabled contributions.
- **Enhance interoperability with regional and NATO partners:** This does not require adopting MDO concepts, but aligning terminology, reporting formats, and liaison structures to ensure that air-enabled effects can be synchronised with other domains.

5.6 Conclusion

MDO reinforces a simple but important truth: effective SFA depends on the ability to generate and integrate effects, not on the possession of specific platforms or domain-centric capabilities. While rebuilding a partner nation's air force remains a long-term, institutionally focused endeavour largely unchanged by MDO, the use of airpower to support the

delivery of SFA is directly shaped by the multi-domain environment. Airpower's ability to sense, connect, move, and protect makes it a critical enabler of SFA activities, provided that its cross-domain dependencies are understood and managed, whether by the supported nation or temporarily by NATO. By adopting an effects-based, domain-agnostic approach, SFA practitioners can better leverage the Air Domain's contributions and ensure that SFA remains coherent, resilient, and effective in contemporary operational context.

Chapter 6 — Cyber Domain

Of all the domains examined in this paper, the cyber domain presents the most compressed timeline between theoretical challenge and operational consequence. When NATO recognised cyberspace as an operational domain at the Warsaw Summit in 2016, it was formalising what partner nations had already been experiencing for years: that digital infrastructure is a legitimate — and frequently targeted — dimension of conflict, one that does not announce itself in advance and does not respect the boundaries between military and civilian systems. The cyber-attacks that preceded and accompanied Russia's aggression in Ukraine, from the BlackEnergy and Industroyer malware campaigns targeting power grids in 2015 and 2016 to the ViaSat satellite network disruption that degraded Ukrainian command and control in the hours before the February 2022 invasion, provided the most operationally consequential case study in cyber warfare that NATO has yet observed in real conditions. They also provided something else: a decade-long laboratory for testing what cyber-focused SFA actually looks like when delivered at scale, under pressure, and against a determined state adversary.

That laboratory is the starting point for this chapter. The contribution developed by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) documents the institutional architecture that NATO and its member states have built to support partner nations' cyber resilience — from the Ukraine Cyber Defence Trust Fund established in 2014 to the Tallinn Mechanism launched in 2023, from the Malware Information Sharing Platform to the Cyber Rapid Response Teams, from the support

extended to Georgia after 2008 to the assistance programmes developed for Moldova and Iraq. Taken together, these mechanisms constitute the most developed existing body of cyber SFA practice within the Alliance, and the Ukrainian experience demonstrates both what sustained cyber capacity building can achieve and what it cannot substitute for. Institutional reform and technical assistance can strengthen a partner nation's cyber resilience substantially. They cannot, on their own, close the asymmetry between a partner nation's cyber maturity and that of the adversary it faces. That gap is not a failure of SFA methodology — it is the most important lesson that cyber SFA has generated.

The lesson carries a corollary that shapes how this chapter should be read. Because the cyber domain is contested continuously rather than episodically, and because its threat picture is renewed faster than any planning cycle can accommodate, cyber SFA cannot be evaluated by the standards ordinarily applied to capability transfer. A partner force equipped with current tools and current expertise is protected only until the next iteration of the threat. What endures is institutional: the capacity to detect, to decide, to coordinate across civilian and military structures, and to revise its own defensive posture without waiting for external direction. This is the argument the contribution below develops through the Alliance's accumulated record — and it is the argument that Chapter 7 extends into the technology that is now reshaping the domain faster than any other.

The Importance of Cyber-Focused Security Force Assistance in Strengthening Partner Nations' Cybersecurity Resilience and Defence Capabilities

Maj. Andrii Davydiuk (UKR), Author

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), PIMEE NAS of Ukraine, SSSCIP of Ukraine

Deputy Branch Head

6.1 Introduction

Cyberspace is a constant battleground, and NATO and its allies face a barrage of cyber threats every day, from low-level attacks to extremely sophisticated incidents. NATO experiences hundreds of cyber incidents every month. These attacks range from phishing attempts and malware infections to more sophisticated and targeted cyber espionage operations. The nature of these cyber threats can vary greatly, and not all incidents result in successful breaches or significant damage. NATO is constantly working to strengthen its cyber defences and resilience to protect its networks and member states from these persistent threats. These malicious cyber activities aim to disrupt NATO's critical infrastructure, disrupt government services, harm society, steal intellectual property, gather intelligence and disrupt military operations[200].

[200] Strengthening cyber resilience 2024: NATO's Cyber coalition and collective defense.

Engagement with Partner countries is based on shared values and common approaches to cyber defence. Requests for cooperation with the Alliance are considered on a case-by-case basis. NATO also cooperates, in particular, with the European Union (EU), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE).

In today's security environment, cyberspace has become a key arena for state and non-state actors. Cyber threats are used to achieve strategic objectives without direct military intervention. In this context, Cyber- SFA becomes particularly important to strengthen the cyber resilience and defence capabilities of partner countries.

Cyber-oriented SFA should include the development of national cyber strategies, by helping to shape policies and the regulatory framework for ensuring cybersecurity. Also relevant is the issue of improving the skills of personnel. Education and training for military and civilian cybersecurity specialists play a special role[201].

NATO conducts regular exercises, such as the annual Cyber Coalition Exercise, and aims to integrate cyber defence elements and considerations across the Alliance's range of exercises, including Crisis Management Exercises (CMX). NATO is also expanding its training and education capabilities, including the NATO Cyber Range, which is based at a facility provided by Estonia.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, is a NATO-accredited multinational and interdisciplinary cyber defence centre of recognised expertise, focusing on

[201] Exercises. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.

cyber defence education, advice, lessons learned, research and development. It is not part of the NATO command structure.

The NATO Communications and Information Academy (NCI) in Oeiras, Portugal, trains personnel from member countries (as well as non-NATO countries) in the operation and maintenance of NATO communications and information systems. The NCI Academy also offers training and education in cyber defence.

The NATO School in Oberammergau, Germany, provides cyber defence education and training to support Alliance operations, strategy, policy, doctrine and procedures.

The NATO Defence College in Rome, Italy, promotes strategic thinking on political-military issues, including cyber defence.

NATO has a number of practical tools to improve situational awareness and facilitate information sharing, including points of contact with national cyber defence authorities in all Alliance capitals. A dedicated Memorandum of Understanding (MOU) defines mechanisms for sharing various cyber defence-related information and providing assistance to improve cyber incident prevention, resilience and response capabilities.

Technical information is also shared through the NATO Malware Information Sharing Platform (MISP), which allows for the rapid exchange of indicators of compromise among Alliance cyber defenders, strengthening the Alliance's overall defence posture.

Of course, developing cyber capabilities in each country is a complex task. According to the Warsaw Summit communiqué[202], Allies “committed to

[202] NATO 2016 Warsaw Summit (2016, July 8).

strengthening the cyber defence of their own national networks and infrastructures as a matter of priority." They will improve their national capabilities to respond to cyberattacks, including in hybrid contexts, and NATO capabilities will undergo "continuous adaptation." It is unclear what the interesting introduction of hybrid contexts into this commitment actually entails. Allies are also "expanding the capabilities and scale of NATO's cyber range."

The communiqué goes on to refer to another document approved at the summit, the "Commitment to Cyber Defence", which states that Allies will "ensure that the Alliance does not lag behind the rapidly evolving cyber threat environment". In it, Allies stipulate that they will prioritize the development of "the fullest range of capabilities to protect national networks and infrastructures", meaning that cyber defence will be considered at the "highest strategic level" at the national level, and that it will be further integrated into operations and its scope will be extended to deployable networks.

The division of labour on cyber defence, with NATO defending its own systems and member states defending theirs, remains, but the commitment emphasizes "accelerating the implementation of agreed cyber defence commitments, including those national systems on which NATO depends." Progress on the pledge will be monitored through an annual assessment based on agreed indicators and will be reviewed at the next summit.

The cyber defence pledge was taken alongside the commitment to strengthen resilience, in which Allies reaffirm their defence investment commitments made at the Wales Summit. Increased defence investment is

seen as key to increasing resilience, as is the protection of supply chains. These guidelines are fully relevant to cyber defence[203].

The summit documents emphasize the importance of cooperation in the field of cyber defence, both among Allies and with third countries and other parties. Only Jordan is mentioned separately in the communiqué (paragraph 106), but it can be assumed that other countries will receive assistance from NATO in cyber defense. For example, Ukraine will receive a Comprehensive Assistance Package (CAP), in accordance with the Joint Statement of the NATO-Ukraine Commission at the level of Heads of State and Government.[204], and although cyber defence is not mentioned in the statement, it is likely that the package will include it. A few weeks before the Summit, the Minister of Defence of Ukraine presented the Ukrainian Strategic Defence Bulletin to NATO Defence Ministers[205] [206] [207]The bulletin discusses the planned reform of the Armed Forces of Ukraine to move towards NATO standards, particularly in the area of cyber defence. This issue is also being addressed by the trust funds established after the Wales Summit.

Much attention was also paid to cooperation between NATO and the EU. The parties signed a Joint Declaration[208], in which cybersecurity and cyber

[203] CCDCOE 2016, The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.
[204] Joint statement of the NATO-Ukraine commission at the level of heads of state and government.
[205] NATO 2016, steps up support for Ukraine with a comprehensive package of assistance. (2016, June 15). NATO.
[206] Ukrainska Pravda, 2016, July 11. The turning point for Ukrainian military reform: What is the strategic defence bulletin and why is it so important?
[207] On the Strategic Defence Bulletin of Ukraine, Decision of the National Security and Defence Council of Ukraine, 2021 (Ukraine).
[208] NATO 2018 Joint declaration on EU-NATO cooperation.

defence are clearly listed among the main topics. On February 10, 2016, a Technical Agreement was signed[209]between the NATO Computer Incident Response Centre (NCIRC) and the European Union Computer Emergency Response Team (CERT-EU) (the text is not available to the public). According to Finnish Yle TV news[210], NATO and the EU considered the possibility of creating a centre for defence against hybrid threats, which was established in 2017[211].

The organizations could also share some of their technical tools and assets, such as NATO's Cyber Range or the NATO Cyber Information and Incident Coordination System (CIICS). EU countries already provide personnel and resources to the NATO CCD COE, demonstrating that they value cooperation with NATO members in the field of cyber defence.

NATO's Industrial Cyber Partnership was also noted in the communiqué and continues to be an important initiative for the Alliance.

After the Russian aggression in 2014, Ukraine became the target of numerous cyberattacks. In response, NATO and other international partners have provided significant assistance in strengthening the country's cyber capabilities. In particular, in 2014, NATO established the Cyber Defence Trust Fund for Ukraine, which provides support for the development of technical capabilities, including laboratories for investigating cybersecurity incidents.[212].By 2016, eight countries had

[209] NATO 2016, and the European Union enhance cyber defence cooperation. (February 10).
[210] Cyber security expert: EU and NATO co-operation pledge bodes well for Finland.
[211] About us - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats.
[212] Townsend, K. (2017, July 11). NATO providing cybersecurity equipment to Ukraine NATO takes steps to bolster Ukrainian cyber security.

contributed a total of €965,000, as well as providing material assistance.[213] [214] [215].

Against the backdrop of the initial stages of Russia's war against Ukraine – not only the illegal annexation of Crimea in 2014, but also the use of cyberattacks, disinformation and other hybrid actions in the years that followed – the NATO-Ukraine Platform on Countering Hybrid Warfare was established at the NATO Summit in Warsaw in July 2016. It provides a mechanism for better identification of hybrid threats and capacity-building to identify vulnerabilities and strengthen the resilience of the state and society. Projects are ongoing to support research, training and expert advice focused on lessons learned, countering disinformation and increasing resilience.[216].

Also in this context, NATO launched the CAP in 2016 as a key mechanism to help Ukraine transform its security and defence sector. This included strategic-level advice through the NATO Mission to Ukraine and NATO Headquarters in Belgium, as well as practical support through a range of capacity-building programmes and initiatives.

In the years leading up to Russia's full-scale invasion in 2022, these reforms helped strengthen Ukraine's ability to defend itself. Through CAP initiatives, NATO members helped Ukraine strengthen its defence capabilities in many areas, including cyber defence, logistics, explosive ordnance disposal, military training and education, and countering hybrid

[213] UKRAINE cyber defence. (2016, June).
[214] Trust funds in support of Ukraine.
[215] Following Notpetya NATO increases support for Ukraine's cyber defences. Security Affairs.
[216] NATO 2025, Relations with Ukraine. (2025, March 11).

threats such as sabotage of critical infrastructure and disinformation campaigns. All of this enhanced Ukraine's ability to resist Russian aggression, which launched a full-scale invasion in February 2022.

At the Vilnius Summit in 2023, Allies agreed to continue developing the CAP into a multi-year assistance programme for Ukraine, based on sustainable and predictable funding. Long-term support is organised around three main pillars: recovery and reconstruction, institutional transformation and transition to NATO interoperability[217] [218].

The Cyber Defence Trust Fund, led by Romania and implemented by the Romanian state-owned company Rasirom, is also supporting Ukraine in developing its defence capabilities in the field of responding to cybersecurity incidents. The assistance includes the establishment of two incident management centres to monitor cybersecurity events, as well as laboratories to investigate and handle cybersecurity incidents. Training on the use of this technology and equipment is also being conducted in Ukraine. In June 2017, the equipment was successfully delivered to Ukrainian beneficiary institutions [219] [220]. In addition, Ukraine has become the main beneficiary of the Science for Peace and Security (SPS) Cooperation Programme. In 2014, NATO allocated €2.2 million for SPS

[217] Comprehensive assistance package 2025 (CAP) for Ukraine. (February 18, 2025). NATO.

[218] FACT SHEET 2016: US and NATO efforts in support of NATO partners, including Georgia, Ukraine, and Moldova. (July 9 2016).

[219] NATO's support to Ukraine. 2018, November.

[220] International cooperation for critical information infrastructure protection: NATO-UKRAINE trust fund on cyber defence. Home - Critical Infrastructure Protection & Resilience Europe.

cooperation with Ukraine, contributing to a projected total of €10 million in 2014-2017.[221].

It is also worth noting that currently, in order to support Ukraine, a new tool for cooperation in the field of cybersecurity - the Tallinn Mechanism - has been created with the participation of the Ministry of Foreign Affairs of Ukraine, Canada, Denmark, Estonia, France, Germany, the Netherlands, Poland, Sweden, the United Kingdom and the United States of America. This step strengthens the interaction of partner countries in the cyber sector against the backdrop of countering Russian aggression against Ukraine. The introduction of the mechanism is the result of joint work of the Ministry of Foreign Affairs, the National Coordination Centre for Cybersecurity, the Ministry of Digital Transformation of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine and other involved entities of cybersecurity of our state. Within the framework of the Tallinn Mechanism, assistance to Ukraine will be coordinated to support and strengthen national cybersecurity and cyber resilience, protect Ukraine's critical infrastructure and prevent Russian cyber operations. The new international instrument will also complement existing international efforts to build cyber resilience and cyber protection of Ukraine's civilian infrastructure. In addition to partner states, non-governmental organizations and the private sector are invited to participate in the Tallinn Mechanism[222]. Another international initiative to support Ukraine is IT

[221] Spinu, N. (2020). Ukraine cybersecurity governance assessment.
[222] Tallinn Mechanism, 2023: Ukraine and international partners launched a new tool for cyber cooperation.

Coalition. The IT Coalition, led by Estonia and Luxembourg, is one of 8 capability coalitions within the Contact Group on Defence of Ukraine. The coalition aims to provide support to the Ministry of Defence and the Armed Forces of Ukraine in the areas of IT, communications and cybersecurity. The Coalition currently includes 14 partner countries and Ukraine. Finland and Spain joined the Coalition in September. It is expected that several more countries will soon become members. Since its establishment in September 2023, the IT Coalition has accumulated 157 million euros in support of Ukraine. In particular, 70 million contributions, including an announced contribution of 10 million from the Netherlands, as well as 87 million from Germany in the form of SAP licenses. Of this amount, Ukraine received equipment and software worth 99 million[223]. Ukraine was also accepted as a contributing participant to NATO CCDCOE. Ukraine's presence at the Centre has enhanced the exchange of cyber expertise between Ukraine and CCDCOE member states. Ukraine provides valuable first-hand knowledge of several adversaries in cyberspace, which is used for research, exercises, and training.[224]

The Washington Summit Declaration, adopted in July 2024, also paid some attention to hybrid threats that pose a challenge to the Alliance. The term hybrid is mentioned 10 times, and Russia is again accused of conducting various types of hybrid operations against NATO members. The Declaration lists sabotage, acts of violence, provocations on the Alliance's borders, the use of weapons of illegal migration, malicious cyber activities,

[223] To support Ukraine, the IT Coalition has successfully accumulated €157 million. (2024, October 16).

[224] CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.

electronic interference, disinformation campaigns and hostile political influence, as well as economic coercion as key Russian hybrid activities that pose a threat to the Alliance's security. The Summit Declaration emphasizes that these Russian hybrid actions will not undermine the resolve and support of Allies for Ukraine, and that the Alliance will provide support to its partners who are most affected by Russia's destabilizing efforts. An issue that has attracted even more attention than hybrid warfare in this official NATO summit declaration and communiqué is the issue of cyber threats and challenges. While the term "hybrid" is mentioned 83 times, the term "cyber" appears 176 times, indicating the Alliance's concern about the impact of such operations on cyberspace. Russia's illegal occupation of Crimea, followed by various types of hybrid anti-NATO operations, as mentioned in official NATO statements, has forced the Alliance to pay more attention to the issue of how to increase the level of resilience in member states. The term "resilience" is mentioned 76 times in NATO documents issued after 2014, starting with the 2014 Wales Summit Declaration and ending with the 2024 Washington Summit Declaration [225]. Having examined in more detail NATO declarations and communiqués from 2002 to 2024, we can conclude about the importance of the cyber domain in the interaction of alliance countries and partners based on the number of mentions in the texts of declarations and communiqués [226].

[225] Godzimirski, J., Bârgăoanu, A., & Ceuca, R. (2024). FLANKS 2, addressing the challenge of the Russian hybrid warfare the NATO way. the case of Norway and Romania. NewStrategy Centre & Norwegian Institute of International Affairs.
[226] NATO summits. (2025, May 2).

NATO Declaration and Communique	Cyber
2002 Prague Summit Declaration	1
2006 Riga Summit Declaration	1
2008 Bucharest Summit Declaration	5
2009 Strasbourg Kehl Summit Declaration	8
2010 Lisbon Summit Declaration	11
2012 Chicago Summit Declaration	10
2014 Wales Summit Declaration	19
2016 Warsaw Summit Communique	23
2018 Brussels Summit Declaration	25
2018 Brussels Summit Communique	25
2022 03 24 NATO Statement	3
2022 Madrid Summit Declaration	7
2023 Vilnius Summit Communique	28
2024 Washington Summit Declaration	10
Total 2002-2024	**176**

Table 1: number of cyber mentions in the texts of declarations and communiqués from 2002 to 2024, for a total amount of 176

In addition to cyber-focused support to Ukraine, NATO is actively involved in developing the cyber capabilities of other Partner countries. In particular, after the cyber-attacks in 2008, Georgia received support from the international community to create a national cybersecurity strategy and develop relevant institutions. In particular, NATO sent a cybersecurity expert to provide assistance and also activated cybersecurity mechanisms developed after the Riga Summit in 2006.[227]. Allies approved the Substantial NATO-Georgia Package (SNGP) at the Wales Summit in

[227] The current situation in Georgia and implications for our policy, US Government Publishing Office.

September 2014 to strengthen Georgia's defence capabilities and assist Georgia in its preparations for Alliance membership. The SNGP builds on NATO's already extensive cooperation through the DEEP, the Building Integrity Programme (BIP) and the Professional Development Programme (PDP), introducing new areas of activity that include:

NATO Core Group and NATO Liaison Office (NLO): The United States provides seconded personnel to support both of these institutions, which offer strategic-level advice on defence matters. Americans have taken on the positions of Deputy Head of the Core Group and Chief Officer of the NLO. Advisory support: Both resident and non-resident NATO experts provide advice on a range of defence issues to enhance the capabilities and interoperability of the Georgian armed forces. Areas of support include acquisition, strategic and operational planning, military police and strategic communications.

Recurrent exercises: Allies support and contribute to NATO exercises that are open to partners and are held in Georgia on a regular basis. The United States linked the AGILE SPIRIT 2015 exercise to NATO, and NATO conducted a computer-based exercise in Georgia in November 2016.

Joint Training and Evaluation Centre (JTEC): Established in 2015, JTEC provides training, evaluation, and certification capabilities to enhance interoperability and operational readiness.

Logistics Facility: NATO is assisting Georgia in building its logistics capacity, which will facilitate the participation of Allies and Partner countries in exercises and disaster relief operations, and will provide support for cargo and personnel involved in NATO-led operations.

School of Defence Institution Building: Building on the experience of DEEP, BIP and PDP, Allies are working with Georgia to establish a centre that will provide classroom and on-the-job training for Georgian government personnel.

Further practical cooperation within the SNGP: At the Warsaw Summit, Allies agreed to strengthen and deepen cooperation with Georgia across a range of efforts, as well as to intensify high-level political dialogue with Georgia[228].

In 2022, the UK announced a new phase of cybersecurity support to Georgia, providing over £5 million to strengthen the country's capabilities to counter cyberattacks from Russia and other threats[229].

In June 2015, Allies agreed to develop a phased DCB package for Moldova. The United States is leading Phase I, which offers advice and assistance from NATO's Defence Reform Expert Group to develop a new National Security Strategy, National Defence Strategy, and National Military Strategy. Moldova completed the development of its new National Security Strategy in June and intends to complete its National Defence Strategy by the end of 2016 and its National Military Strategy in 2017. Phase II will provide assistance and advice on the development of Moldova's land and air forces, command and control, training doctrine and infrastructure, cyber defence and military education, and will help fight corruption.

[228] FACT SHEET: US and NATO efforts in support of NATO partners, including Georgia, Ukraine, and Moldova.

[229] Prime Minister's Office, 10 Downing Street. (2022, June 29). New UK support to protect Georgia against Russian cyber attacks.

In addition to strong support for Ukraine, Georgia and Moldova, Allies are providing support to a number of countries in the Middle East and North Africa, including but not limited to Iraq, Jordan and Tunisia. In July 2015, NATO approved a DCB package for Iraq to strengthen its defence capabilities, reform its security sector and increase its capacity to contribute to regional security.

Another excellent example of developing support from NATO countries and partners is Estonia, which, after a large-scale cyberattack in 2007, became a leader in cybersecurity by establishing the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and actively sharing its experience with other countries.[230].

6.2 Addressing Cyber Threats, Securing Communication Networks, and Sharing Intelligence

The global security situation is becoming increasingly complex as Russia employs a variety of tactics, including hybrid warfare, cyberattacks and conventional military operations. NATO's response is focused on strengthening intelligence, surveillance and reconnaissance (ISR) capabilities to better understand and counter these multifaceted threats[231].

In today's security environment, cyber threats have become an integral part of hybrid conflicts. NATO countries and partners, including Ukraine, are

[230] About us. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.

[231] Can NATO's intelligence and surveillance enhancements turn the tide in Ukraine? - defence domain. Home - Defence Domain.

subject to constant cyberattacks aimed at destabilizing their information systems and critical infrastructure.

Intelligence sharing has long been a cornerstone of military alliances, allowing nations to pool resources, improve situational awareness, and coordinate strategic responses to common threats. However, as global security challenges become increasingly complex and technologically advanced, the processes and systems that underpin intelligence sharing must evolve to keep pace. Today's threats, including cyberattacks, terrorism, and great power competition, require faster, more accurate, and more secure mechanisms for sharing critical information.

Intelligence sharing plays a key role in building trust and cohesion in military alliances. By combining information from different sources, allies can gain a more complete understanding of threats, reducing blind spots and improving decision-making. This collaborative approach also helps to spread the burden of intelligence collection, allowing countries with different capabilities and geographic focus to contribute to a shared security system.

For alliances such as NATO, the Five Eyes (FVEY) and the European Union (EU), intelligence sharing is essential to achieving collective defence objectives. During the Cold War, for example, intelligence cooperation between Western allies provided critical insight into the activities of the Soviet Union, enabling a coordinated response to geopolitical events. Today, intelligence sharing remains a cornerstone of collective security, helping allies counter a wide range of threats, from terrorism and cyberwarfare to regional aggression and global pandemics

[232]. In response to these threats, NATO has stepped up intelligence sharing and strengthened cyber defence. In particular, NATO and Ukraine signed an agreement on enhanced cyber cooperation, which provides for Ukraine's access to the Malware Information Sharing Platform (MISP[233])[234].

Technological advances are driving significant changes in how intelligence is shared between military alliances. These innovations are increasing the speed, accuracy, and security of information exchange, making them more effective in countering modern threats.

One of the most transformative developments is the integration of artificial intelligence (AI) and machine learning into intelligence analysis. These technologies allow us to quickly process vast amounts of data, identifying patterns and anomalies that would be difficult or impossible for analysts to detect. For example, AI can analyse satellite imagery to identify troop movements or detect cyber intrusions in real time, providing operational intelligence to allied decision-makers. Big data analytics also plays a crucial role in modern intelligence sharing. By collecting and analysing information from diverse sources such as social media, sensors, and human intelligence, big data tools provide a holistic view of the operational environment. This capability is particularly valuable during counterterrorism operations, where timely and accurate intelligence can

[232] The evolution of intelligence sharing among military alliances. Genesys Defence and Technologies.
[233] MISP threat intelligence platform & open standards for threat information sharing. (n. d.). MISP Threat Intelligence Platform & Open Standards For Threat Information Sharing.
[234] Statement by the NATO Secretary General on cyber attacks against Ukraine. NATO.

mean the difference between preventing an attack and responding to its consequences [235].

The NATO Intelligence, Surveillance and Reconnaissance Force (NISRF) is an integral part of NATO's ability to collect, process and disseminate intelligence across a range of domains, including land, sea, air, space and cyber. The ongoing war in Ukraine has shown that effective intelligence is essential to understanding and countering Russian military operations, which are often characterised by rapid and unpredictable manoeuvres in these domains.

Effective intelligence sharing is a key element in countering cyber threats. NATO is actively working with Partner countries to improve information sharing on cyber threats. NATO is also considering expanding cooperation with Ukraine in the area of intelligence sharing on Russian electronic warfare (EW)[236].

NISRF works closely with the command structure, NATO force structure and national intelligence networks, ensuring a coordinated and comprehensive response to threats. During the conflict in Ukraine, NISRF provided critical intelligence that was essential to supporting Ukraine's defence and informing NATO's strategic decisions.

The Alliance Future Surveillance and Control (AFSC) program is designed to replace NATO's aging Airborne Warning and Control System (AWACS), which has been vital in monitoring Russian air operations during the conflict in Ukraine. AFSC aims to develop a more integrated

[235] The evolution of intelligence sharing among military alliances. Genesys Defence and Technologies.

[236] NATO eyes intelligence sharing with Ukraine on Russia's EW capabilities. The Defence Post.

and adaptable surveillance and control system that incorporates advanced technologies such as artificial intelligence and big data analytics to improve situational awareness and decision-making. By integrating air, space and cyber surveillance, AFSC directly supports NATO's efforts in Ukraine, providing enhanced capabilities essential for early warning and threat detection. This integration ensures that NATO can respond more effectively to Russian air and missile threats, which have been significant in the conflict.

While technological innovations have increased the efficiency and effectiveness of intelligence sharing, they also create new challenges that alliances must address to maintain operational cohesion and trust.

One of the most important challenges is ensuring the interoperability of related systems. Military alliances often include countries with different levels of technological development and different approaches to intelligence gathering. Integrating these disparate systems into a single framework requires standardized protocols, robust training programs, and ongoing updates to maintain interoperability.

Another important issue is ensuring the security of shared intelligence. As cyber threats become more sophisticated, ensuring the integrity and confidentiality of sensitive data becomes increasingly difficult. Adversaries may target communications networks in an attempt to intercept or manipulate intelligence data to sow discord among allies or disrupt their operations. Robust cybersecurity measures, including end-to-end encryption and constant monitoring, are essential to mitigating these risks.

Geopolitical tensions within alliances can also complicate intelligence sharing. Differences in national interests, priorities, and threat perceptions can lead to members being reluctant to share certain types of information. For example, some countries may withhold intelligence to protect sources or avoid revealing sensitive capabilities. Overcoming these barriers requires strong leadership, clear guidance, and mechanisms for resolving disputes.[237].

Furthermore, NATO's reliance on ISR capabilities exposes it to cyber and electronic warfare threats from Russia, which has demonstrated significant capabilities in these areas. Ensuring NATO's ISR systems are resilient to such threats is critical to maintaining their effectiveness. NATO must prioritize robust cybersecurity measures to protect its ISR assets from potential cyber threats [238].

NATO's focus on cyber defence is to protect its own networks, to operate in cyberspace (including through Alliance operations and missions), to help Allies increase their national resilience, and to provide a platform for political consultation and collective action. The NATO Cyber Security Centre (NCSC), based at the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium, protects NATO's own networks by providing centralised, 24/7 cyber defence support. This capability is constantly evolving and keeps pace with the rapidly changing threat and technological environment. NATO has also established a Cyberspace Operations Centre in Mons, Belgium. The centre provides situational awareness support to

[237] The evolution of intelligence sharing among military alliances. Genesys Defence and Technologies.

[238] Can NATO's intelligence and surveillance enhancements turn the tide in Ukraine? - defence domain. Home - Defence Domain.

military commanders to inform Alliance operations and missions. It also coordinates NATO's operational activities in cyberspace, ensuring freedom of action in this domain and making operations more resilient to cyber threats. To promote a common approach to developing cyber defence capabilities across the Alliance, NATO also sets targets for the implementation of national cyber defence capabilities by Allies through the NATO Defence Planning Process.

Protecting communications networks is critical to ensuring continuity of command and control in the face of cyber threats. Hours before Russian troops crossed the border into Ukraine, cyberattacks hit Ukrainian government agencies, military and emergency services. ViaSat satellite network down. Communications outage for Ukrainian police, military and intelligence agencies. The attack has caused collateral damage beyond Ukraine. It affects wind turbines and disrupts internet access for tens of thousands of people across Europe[239].

Secure communications networks are another key factor in modern intelligence sharing. Encrypted systems, such as those used in NATO's Battlefield Information Collection and Exploitation Systems (BICES), allow allies to exchange sensitive information without fear of interception or compromise. These networks are designed to facilitate real-time collaboration, ensuring that intelligence reaches the right people at the right time[240].

[239] Statement by the NATO Secretary General on cyber attacks against Ukraine. NATO.
[240] The evolution of intelligence sharing among military alliances. Genesys Defence and Technologies.

NATO provides technical support to Partner countries in strengthening their communications systems. As NATO's cyber defender and technology hub, the NATO Communications and Information Agency (NCIA) support the Alliance by providing secure information technology (IT) and cybersecurity services within the NATO enterprise to ensure a resilient environment. NCIA scientists support NATO's resilience in cyberspace by protecting NATO networks and the NATO digital backbone, operating in cyberspace during Alliance operations and missions, and providing a platform for political consultation and collective action by Allies. Cyber threats to the Alliance's security are becoming increasingly frequent, complex, destructive and coercive. A single data breach can have devastating consequences, jeopardizing public security and collective defence. Recognizing this seriousness, NATO is adapting its approach to cyber threats and cybersecurity solutions with thoughtfulness and urgency. By engaging with Allies, industry, academia and leading cyber agencies, NATO has a high level of cyber threat awareness and can respond effectively and efficiently to malicious cyber activity. NCIA's cybersecurity work can be divided into four categories: cyber adaptation, digital modernization, cybersecurity and cyber training. Following the Russia-Ukraine conflict, NATO cooperation with Ukraine has intensified since 2014, particularly in critical areas. The NATO Communications and Information Academy (NCI Academy) is contributing to the Alliance's initiative to share knowledge and expertise in command, control,

communications and computers (C4) to help Ukraine build its own reliable and resilient CIS capabilities[241].

Also, in 2018, NATO transferred to Ukraine secure communications equipment, which is still in use.[242]. Finally, improvements in space-based capabilities are improving intelligence sharing, providing global coverage and real-time surveillance. Satellites equipped with advanced sensors and communications systems allow for the collection and dissemination of critical information over long distances, supporting a coordinated response to transnational threats.

The evolution of intelligence sharing between military alliances reflects the increasing complexity of today's threats and the transformative potential of technology. By leveraging artificial intelligence, big data analytics, secure communications networks, and space-based capabilities, alliances can improve the speed, accuracy, and security of their intelligence-sharing efforts. However, addressing challenges such as interoperability, cybersecurity, and geopolitical tensions will be critical to maintaining trust and unity among allies.

6.3 A Relevant Case Study and Best Practice

Since 2014, Ukraine has been the target of numerous cyberattacks, accompanied by hybrid threats from the Russian Federation. Despite this, the country has demonstrated significant cyber resilience, which was made possible by domestic reforms and international support, including from NATO.

[241] Knowledge sharing with Ukraine gains momentum. (2017, June 23).
[242] NATO 2022 Agency and Ukraine reaffirm commitment to technical cooperation.

After the annexation of Crimea and the start of the conflict in eastern Ukraine, the country focused on strengthening its cyber capabilities. A national cybersecurity strategy has been developed, and legislative changes have been implemented to strengthen cyber defence. These measures have allowed Ukraine to respond more effectively to cyberattacks and reduce their impact on critical infrastructure.

NATO has played a key role in supporting Ukraine in the field of cybersecurity. In particular, the Cyber Defence Trust Fund was established to provide technical assistance and promote the development of Ukraine's institutional capacity in the field of cybersecurity. In addition, Ukraine became a member of the Malicious Information Sharing Platform, which allowed for more effective exchange of information on cyber threats with NATO partners.

By studying cyberwarfare, we can gain insight into the innovations and challenges that define cybersecurity in modern defence. Cyberwarfare tactics have evolved significantly, with state and non-state actors using increasingly sophisticated methods to disrupt and harm military operations. For the Armed Forces of Georgia and Ukraine, cyberattacks have become a constant threat that requires constant vigilance and adaptation.

In 2008, during the Russian invasion of Georgia, the Georgian military suffered a coordinated cyberattack that paralyzed government websites and disrupted communications. This attack, considered one of the first cases of cyberwarfare accompanying kinetic military operations, highlighted the vulnerability of digital infrastructure. The attackers used distributed denial-of-service (DDoS) attacks, disrupting websites and spreading disinformation. These tactics not only hampered Georgia's military

response but also sowed confusion and panic among the civilian population.

Ukraine has faced similar, if not more serious, challenges since the annexation of Crimea in 2014 and the ongoing invasion of eastern Ukraine. Ukrainian military and government networks have been the target of a series of cyberattacks attributed to Russian-backed hackers. Notable incidents include attacks on Ukraine's power grid in 2015 and 2016, which caused massive power outages and highlighted the potential for cyberattacks to cause real damage. The malware used, known as BlackEnergy and Industroyer, demonstrated a high level of sophistication and the ability to target industrial control systems.

These examples illustrate how cyberwarfare tactics have evolved to include not only disruptive attacks on websites and networks, but also more disruptive operations targeting critical infrastructure. For the military, this requires a comprehensive approach to cybersecurity that can protect against a wide range of threats. In response to the growing cyber threat, the military has invested in and developed innovative cybersecurity tools. Both Georgia and Ukraine have made significant progress in strengthening their cyber defence capabilities, often with the support of international partners. The Georgian Armed Forces, recognizing the importance of robust cybersecurity, have established a dedicated Cyber Security Bureau within the Ministry of Defence. This bureau is responsible for protecting military networks, conducting cyber threat analysis, and developing defence strategies. In addition to strengthening domestic capabilities, Georgia has also benefited from cooperation with NATO and the European Union,

which have provided training, resources, and expertise to strengthen Georgia's cyber defences.

Ukraine, facing an increased cyber threat, has also made cybersecurity a top priority. Specialized cyber units have been established within the Ukrainian Armed Forces and other defence agencies to protect military networks and respond to cyber incidents. Ukraine has received significant support from the United States and European countries, which have provided technical assistance, training, and advanced cybersecurity tools. One notable initiative is the Ukraine Cyber Defence Cooperation (UCDAC), a collaborative effort to enhance Ukraine’s cyber resilience through knowledge sharing and capacity building.

Technological innovation is playing a critical role in these efforts. Advances in artificial intelligence (AI) and machine learning are being used to more effectively detect and respond to cyber threats. AI-driven systems can analyse vast amounts of data to identify patterns and anomalies that indicate cyberattacks, enabling faster and more accurate threat detection. In addition, the development of advanced encryption technologies is helping to protect sensitive military communications from interception and tampering. Integrating these technologies into military cyber defence strategies is a significant step forward. However, it is important to recognize that technology alone is not a panacea. Effective cybersecurity also requires well-trained personnel, robust policies, and a security-conscious culture within the military.

Indeed, while technological progress is crucial, human factors and organizational issues play an equally important role in cybersecurity. The armed forces of Georgia and Ukraine have faced challenges in training,

coordinating, and integrating cyber defence into broader military strategies. One of the main challenges is the shortage of qualified cybersecurity professionals. Both Georgia and Ukraine face a significant gap in the number of trained cyber experts relative to the scale of the threats they face. This shortage is exacerbated by the fact that qualified professionals are often lured away by higher salaries in the private sector. To address this problem, both countries have implemented programs to develop and retain cyber talent. In Georgia, initiatives such as Cybersecurity Awareness Month aim to educate and train military personnel at all levels, while in Ukraine, cyber academies have been established to educate a new generation of cyber defence experts.

Another important challenge is coordination between different branches of the armed forces and government agencies. Effective cyber defence requires seamless cooperation and information sharing, but bureaucratic obstacles and closed structures can hinder these efforts. For example, in the early stages of the conflict in Ukraine, significant difficulties arose in coordinating cyber defence activities between the military, intelligence services, and civilian authorities. Recognizing this, Ukraine has since made efforts to improve interagency cooperation, including the establishment of a National Cyber Security Coordination Centre to optimize response to cyber incidents.

In addition, integrating cyber defence into an overall military strategy is a complex task. Cyber operations must be aligned with traditional military objectives and tactics, requiring a deep understanding of both domains. In Georgia, integrating cyber defence into military exercises has become a priority, allowing strategies to be tested and refined in simulated

environments. Similarly, Ukraine has incorporated cyber warfare scenarios into its military training programs, ensuring that personnel are prepared for the multifaceted nature of modern conflicts.

The experiences of the armed forces of Georgia and Ukraine underscore the critical importance of cybersecurity in modern defence. As cyberwarfare tactics continue to evolve, militaries must adapt and innovate to protect their digital infrastructure and maintain operational integrity. The challenges they face, from technological complexity to organizational coordination, underscore the complexity of the cyberspace.

Investing in advanced technology, developing skilled personnel, and fostering international cooperation are essential components of a robust cyber defence strategy. As the digital battlefield continues to expand, the lessons learned by Georgia and Ukraine will serve as valuable guidelines for other countries navigating the treacherous landscape of cyberwarfare. The future of defence will undoubtedly be defined by the ongoing struggle to secure cyberspace, which is at the heart of our increasingly interconnected world[243].

It is also worth noting that the evolution of intelligence sharing is evident in several high-profile examples that highlight its importance and impact.

One notable case is the Five Eyes alliance, which includes the United States, the United Kingdom, Canada, Australia, and New Zealand. This long-standing intelligence-sharing network has adapted to modern challenges, integrating advanced technologies and expanding its focus on cyber threats and emerging technologies. The Five Eyes alliance is an

[243] Defence sector review with mercury strategic: Cybersecurity challenges and innovations. Georgia Today.

example of how trust and technological innovation can enhance collective security. Another example is NATO's response to Russia's aggressive war in Ukraine. Intelligence sharing among NATO members is crucial for countering Russian disinformation campaigns, tracking troop movements, and coordinating support for Ukraine. The use of real-time intelligence, supported by satellite imagery and cyber monitoring, has enabled NATO to maintain situational awareness and respond effectively to emerging threats. These efforts underscore the importance of using a variety of intelligence sources to combat complex and adaptive threats[244].

Thanks to the measures taken and international support, Ukraine has been able to increase its cyber resilience. The country effectively counters cyber-attacks, ensures the uninterrupted operation of critical infrastructure, and actively cooperates with international partners in the field of cybersecurity. This experience can serve as an example for other countries seeking to strengthen their cyber capabilities.

NATO helps Allies strengthen their national cyber defences by facilitating the exchange of information and best practices, and by conducting cyber defence training to develop national expertise. Similarly, individual Allies can, on a voluntary basis and with NATO's support, help other Allies develop their national cyber defence capabilities. NATO's Cyber Rapid Response Teams are available 24/7 to assist Allies upon request and approval by the North Atlantic Council.

[244] The evolution of intelligence sharing among military alliances. Genesys Defence and Technologies.

Chapter 7 — Artificial Intelligence as a Cross-Domain Enabler

The integration of effects across domains, which this paper has treated throughout as the defining requirement of Multi-Domain Operations, depends on something that no single domain supplies: the capacity to process information, recognise patterns, and reach decisions faster than an adversary can act. That capacity is now being transformed by artificial intelligence. The Alliance has moved quickly to acknowledge this, integrating an AI-enabled command system into Allied Command Operations in 2025 through an exceptionally rapid procurement, and AI-derived processing already shapes how surveillance data from space is exploited, how anomalous activity is detected in networks, how targeting is supported in the air domain, and how logistics are sustained on land. Artificial intelligence is, in this sense, the connective tissue of multi-domain integration — the means by which effects generated in separate domains are fused into a coherent picture and converted into decision advantage. This has direct consequences for Security Force Assistance. A partner force that cannot exploit AI-enabled processing will not simply be less efficient; it will operate at a different tempo from the Alliance alongside which it is expected to act, and the interface between them — the interface this paper has identified as NATO's most critical — will become the point at which multi-domain coherence breaks down. Conversely, a partner force that fields such systems without the institutions to govern them acquires a dependency rather than a capability. Both outcomes fall within

the remit of SFA, and neither can be addressed by equipment transfer alone.

The contribution that follows, developed by Deloitte Italy, maps the environment in which that effort must now be conducted. It examines the geopolitical competition in AI between the United States, China, and Russia, and what that competition implies for cooperative security frameworks. It assesses the pace of technological acceleration and the accompanying skills transformation — the World Economic Forum estimates that 59 per cent of the global workforce will require reskilling or upskilling by 2030. It analyses the first generation of binding regulatory instruments, notably the EU AI Act and the Cyber Resilience Act, both adopted in 2024, which are beginning to define the governance architecture within which AI and cyber capabilities must be developed and fielded. And it sets out the threat landscape created by AI-enabled offensive capabilities that automate attacks, optimise social engineering, and adapt in contact. Each of these dimensions translates into a concrete institutional requirement for partner nations. Geopolitical competition in AI means that partner forces will increasingly field systems whose provenance, dependencies, and supply chains carry strategic implications that cannot be left to procurement alone. The skills transformation means that the binding constraint on partner AI capability will be human and institutional long before it is technical: a partner nation unable to recruit, train, and retain the expertise to operate and audit these systems will not benefit from acquiring them. The regulatory frameworks, though European in origin, establish a de facto interoperability baseline — partner forces that cannot demonstrate accountable, auditable AI governance will find their ability to

exchange data and operate alongside Allied systems constrained for reasons that are legal rather than technical. And an adversary employing AI-enabled offensive capabilities does not need to outmatch a partner nation across the board; it needs only to find the point at which that partner's detection and response capacity has not kept pace.

These requirements are addressed directly in the recommendations with which the contribution concludes, framed explicitly for partner countries: interoperable cyber risk governance frameworks that embed AI-specific accountability and ethical safeguards; the development of AI-enabled defensive capability; scenario-based planning and strategic simulation; and the cultivation of digital fluency at command level, so that senior leaders can interrogate the systems on which their decisions increasingly rely. Each is an institutional capacity rather than a technical acquisition, and each therefore falls squarely within the remit of Security Force Assistance.

Artificial intelligence compresses the interval between technological change and operational consequence to a point at which programmes calibrated to a fixed capability baseline begin to depreciate before they conclude. The response is not to accelerate capability transfer but to change what is transferred: from proficiency with a given generation of systems to the institutional capacity to govern, adapt, and renew them. That distinction — between building capability and building the ability to sustain capability — is the practical meaning of treating SFA as a structural enabler of Multi-Domain Operations, and Chapter 10 returns to it when considering how the Alliance should resource and measure the effort.

Global Artificial Intelligence and Cyber Trends

Bianca de Teffé Erb (ITA/USA), Author
Deloitte Italy, EMEA AI Risk Leader

David Mach (ITA), Author
Deloitte Italy, Data & AI Ethics Consultant

7.1 Geopolitical and Strategic Shifts

Artificial intelligence's (AI) emergence as a transformative force in modern warfare is reshaping the global geopolitical landscape. Political analysts have gone so far as characterizing these changes introduced by advanced AI as a de facto arms race, led by major powers including the United States, China, and Russia. This perspective underscores the growing strategic relevance of AI as a critical enabler of military and geopolitical influence in an increasingly multipolar international system. This does not only impact NATO's strategic posture but also reinforces the need for cooperative security frameworks to fully grasp the opportunities and mitigate the risks associated with AI proliferation. The April 2025 briefing on Defence and Artificial Intelligence from the European Parliamentary Research Service denotes, for example, the critical role AI has played in the Russian invasion of Ukraine, demonstrating AI's

importance in intelligence gathering, autonomous systems, and Cyber operations. [245]

Thus, it can be highlighted that the geopolitical landscape of AI is marked by strategic competition, with the United States and China positioning themselves as global leaders in AI development, and Russia intensifying its efforts to expand its technological and military capabilities in the field. Recognizing the strategic implications, the European Union (EU) has also moved decisively, to avoid falling behind, embracing the importance and relevance of AI and Cyber in relation to continental defence via the EU Strategic Compass and the European Defence Fund's budget allocation of 4-10% for disruptive technologies and future defence solutions. Furthermore, the EU Defence Innovation Scheme (EUDIS) provides grants and services to private entities to help bring pioneering ideas to the defence sector, which notably includes a technological challenge in AI. [246]

Beyond the EU, the multipolar dynamics of AI development are evident in the strategic investments and policies of the major global powers mentioned above. The United States, for instance, has prioritized AI in its national defence strategies, recognizing its potential to enhance military capabilities and maintain technological superiority. The US Department of Defence (DOD) has established the Joint Artificial Intelligence Center (JAIC) to coordinate AI efforts and develop applications for military use.[247] Similarly, China has identified AI as a strategic priority in its "Next

[245] Defence and Artificial Intelligence. 2025, April. European Parliament.
[246] European Defence Fund 2025: Over €1 Billion to Drive Next-Generation Defence Technologies and Innovation. (Jan, 2025). European Commission.
[247] Joint Artificial Intelligence Center has Substantially Grown To Aid The War fighter. (2020, Nov). US DoD.

Generation AI Development Plan," aiming to become a global leader in AI by 2030. Russia, despite still being a step behind the US and China, has outlined a national strategy to bridge the gap in AI development, focusing on enhancing AI expertise, education, datasets, infrastructure, and regulations.[248]

While it may be tempting, especially in light of the presented scenario, to draw parallels between today's developments in AI and the Cold War–era nuclear arms race, such analogies risk oversimplifying a far more complex and multidimensional phenomenon. The term "AI arms race", which has been previously introduced, has indeed gained traction in political and media discourse, yet it fails to capture the fundamental differences between the current technological landscape and historical military buildups. AI is not a weapon in itself, nor does its development follow a linear, state-centric model of accumulation. Rather, it is a general-purpose technology shaped by a diverse ecosystem of actors (including private industry, academia, and government agencies) driven as much by economic incentives and innovation cycles as by geopolitical considerations.[249] In this chapter, we exactly aim to unpack this complexity by examining how AI intersects with Cybersecurity, defence innovation, and broader systemic transformations that defy traditional metaphors.

This complexity combined with the competitive nature of AI development described above has significant implications for global security. The introduction of AI in military systems can lead to increased autonomy in

[248] Defence and Artificial Intelligence. (2025, April). European Parliament. Ibid.
[249] AI and Arms Races: Technology Development is not Weapons Manufacturing. We Need New Terms for AI Competition. (2025, Jun).

decision-making, faster response times, and enhanced capabilities in intelligence, surveillance, and reconnaissance (ISR). Despite introducing relevant opportunities, it also raises ethical concerns and the potential for conflict escalation. The absence of a unified international regulatory framework further exacerbates these risks, highlighting the need for cooperative security frameworks to ensure responsible governance and oversight of AI technologies and proper consideration of the Cyber implications. Recognizing the strategic importance of AI, NATO adopted a revised AI Strategy in 2024 pledging to harness the technology within set principles of responsibility to promote defence, accelerate AI adoption, safeguard AI technologies, and manage associated risks while countering threats from adversarial AI[250] (Principles of AI Responsible Use or PRUs). In addition, the 2024 revised AI strategy also highlights the collaborative & strategic need for NATO to work with AI stakeholders spanning across industry, academic, non-profit organizations, and non-traditional sectors via trusted funding sources among allied countries at a national and international level.

As a result of the AI & Cyber competitive multipolar landscape displayed so far, NATO's strategic posture would strongly benefit from continued adaptation to the rapid advancements in AI and Cyber capabilities in an ethical manner. AI is, indeed, now integral to intelligence gathering, autonomous systems, and Cyber operations as seen in recent conflicts (e.g., Russia-Ukraine War), necessitating a recalibration of NATO's defence strategies. Throughout time, the Organization's strategic posture has been

[250] NATO Releases Revised AI Strategy. (2024, Jul). NATO.

shaped by its commitment to collective defence and the need to adapt to the evolving security environment. The present circumstances call for a comparable approach. Against this backdrop, a closer look at NATO's AI and Cyber posture provides insight into how the Alliance is positioning itself for the challenges ahead. When it comes to Cyber defence, NATO's approach is currently multifaceted, encompassing the protection of its own networks, the integration of Cyber capabilities into operations and missions, and the enhancement of national resilience among member states.[251] Although predating much of significant advancements of AI technology in recent years, NATO's Cyber Defence Pledge, adopted at the Warsaw Summit in 2016, presents this approach, further underscoring the importance of strengthening national Cyber defences to protect national networks and infrastructures.[252] This encompasses the integration of Cyber defence into NATO operations, the expansion of the Alliance's Cyber range, and the ongoing adaptation of its capabilities to address the rapidly evolving Cyber threat landscape. The latter point naturally links to developments in AI, which present both innovative opportunities and significant threats. AI is increasingly shaping the Cyber domain, compelling NATO to reassess its capabilities, invest in emerging technologies, and refine its strategic approach, as demonstrated, for instance, by the issuance of the PRUs. To align with these changes in the geopolitical and technological panorama and in unison with NATO SFA's own mandate to support security forces in partner countries via knowledge

[251] NATO Releases Revised AI Strategy. 2024, Jul, op. cit.
[252] Strengthening Cyber Resilience 2024: NATO's Cyber Coalition and Collective Defence. NATO Strategic Warfare Command.

sharing,[253] the Warsaw pledge & NATO's revised AI Strategy emphasize the importance of cooperation among Allies and with partner countries, recognising that AI & Cyber threats are global in nature and require a coordinated response.

The Alliance has established practical tools to improve situational awareness and facilitate information sharing, including points of contact with national Cyber defence authorities in all Alliance capitals. A dedicated Memorandum of Understanding (MOU) defines mechanisms for sharing various Cyber defence-related information and aiding to improve Cyber incident prevention, resilience, and response capabilities.[254] Technical information is also shared through the NATO Malware Information Sharing Platform (MISP), which allows for the rapid exchange of indicators of compromise among Alliance Cyber defenders, bolstering the Alliance's complete defence posture.[255] The division of labour on AI & Cyber defence, with NATO defending its own systems and member states defending theirs may remain, but the Alliance's collective security commitments emphasize progress and NATO's strategic approach to AI & Cyber should continue on this collective path for success.

7.2 Technological Acceleration and Future Skills Landscape

The convergence of AI and Cyber technologies presents risk and opportunity in military and security contexts. Emerging technologies,

[253] NATO Centres of Excellence 2023 – Security Force Assistance (SFA). NATO Strategic Warfare Command.
[254] Cyber defence. (2024, Jul). NATO OTAN.
[255] Cyber defence. (2024, Jul). NATO OTAN. Ibid.

spanning across the two domains, such as autonomous systems, machine learning, and quantum computing are rapidly advancing, offering not only enhanced capabilities in ISR, as mentioned above, but potentially impacting logistics and broader Cyber operations. These innovations, hence, necessitate to re-think and update military doctrines, strategies, and organisational structures to fully harness their potential while reducing risks. As such, NATO has adopted a forward leaning posture with the 2022 launch of the Defence Innovation Accelerator for the North Atlantic (DIANA) Network that aims to bolster transatlantic defence innovation through the harnessing of cutting-edge technologies and fostering collaboration among allied countries for collective defence and security.[256] NATO DIANA's current efforts have included 23 accelerators across the alliance, 182 test centres, and an investor network within the Allied Capital Community for trusted third party funding of dual-use technology solutions. The 2021 NATO Innovation Fund also accelerates advanced technological adoption via strategic investments in start-ups creating dual-use disruptive technologies with a total of EUR 1 billion in available funds.[257] These efforts, going beyond mere policy statements, highlight NATO's commitment to foster a collaborative and proactive approach to AI, Cyber and Collaboration. NATO's investments to technological innovation are echoed by other major internation cooperation entities. For instance, the 2025 European Parliament briefing also denotes the significance of AI-powered defence innovation and additional initiatives, noting that multiple European Defence Fund and Permanent Structured

[256] Defence Innovation Accelerator for the North Atlantic. (2025, Jun). NATO DIANA.
[257] NATO Innovation Fund. (IF).

Cooperation (PESCO) projects are dedicated to integrating AI into future military capabilities.[258]

Among the most critical technologies that have emerged in recent years, autonomous systems, such as drones and unmanned vehicles, are among the most effective for reconnaissance, logistics, and combat operations, reducing risk to human personnel and enhancing operational efficiency through AI. Further, machine learning algorithms analyse vast amounts of data, providing insights for strategic decision-making and situational awareness. Finally, quantum computing is rapidly emerging offering unprecedented computational power and security, ideal for tasks such as codebreaking, optimisation, and simulation. Cyber operations disrupt enemy communications, degrade infrastructure, and gather intelligence, with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, facilitating collaboration among NATO members and partners.

Most visible in the public domain due to its universal and cross-sectional impact, AI plays an increasingly important role in Cyber defence, detecting and responding to Cyber threats in real-time. Blockchain technology enhances security and transparency for data transactions, securing communications, protecting sensitive information, and ensuring data integrity. The Internet of Things (IoT) connects devices, sensors, and systems to enhance situational awareness and operational efficiency and 5G technology provides faster, more reliable, and secure connectivity, enhancing capabilities in areas such as real-time video streaming, remote

[258] Defence and Artificial Intelligence. (2025, April). European Parliament. Ibid.

control of unmanned systems, and secure communications. NATO currently groups many of these technologies under its emerging and disruptive technologies (EDT) strategy to ensure allies are fostering the development of new technologies while trying to mitigate their use against members of the alliance.[259] NATO has embraced a comprehensive strategy by collaborating with the private sector and academia to integrate EDTs, ensuring it retains its operational and tactical superiority while proactively considering the potential threats these technological advancements may pose.

As technology continues to advance, it is essential to keep people at the centre of these developments. While upholding IHL and fundamental rights remains non-negotiable, it is equally important that individuals understand the nature of the challenges they face. They must be equipped not only to navigate and effectively use emerging technologies, but also to exercise sound judgment in knowing when their use should be paused or slowed. However, the pace of technological evolution, particularly in the fields of AI and Cyber, demands that future skills align closely with the digital transformation of security forces. This calls for an adaptable approach that is both dynamic and easy to replicate or modify.

As AI and Cyber capabilities become increasingly integrated into the defence and security sectors, it is clear that not all personnel can, or need to, be technical experts. While in-depth knowledge of autonomous systems, machine learning, quantum computing, and Cyber operations is essential for certain specialised roles, it is not practical nor necessary for

[259] Emerging and disruptive technologies. (2024, Aug). NATO.

every professional to master these complex domains. However, a foundational understanding of AI, Cybersecurity, and related technologies is rapidly becoming a baseline requirement across all functions. According to the Future of Jobs Report 2025, nearly 40% of the core skills required on the job are expected to change by 2030, and 59% of the global workforce will require reskilling or upskilling to remain effective in their roles.[260] This includes not only technical training but also the capacity to interact intelligently and ethically with advanced technologies.

Crucially, the report emphasizes that future skill demands will blend both technical and human competencies. While roles in AI, big data, and Cybersecurity are among the fastest-growing, skills such as resilience, leadership, analytical thinking, and collaboration are equally vital. In military and security environments, where ethical decisions must often be made under pressure and within complex operational contexts, this dual skillset becomes indispensable. Developing AI and Cyber literacy is not solely about operating systems or analysing data, it is about understanding the strategic, ethical, and legal implications of their deployment in real-world combat scenarios, particularly in high-stakes contexts such as autonomous systems or surveillance operations.

Therefore, cultivating AI ethics within the armed forces and security sectors requires dismantling traditional knowledge silos. The report stresses that generative AI and other technological shifts are "upending industries and labour markets" and require a "collective response" across government, business, and education to address both the opportunities and

[260] Future of Jobs Report 2025: 78 Million New Job Opportunities by 2030 but Urgent Upskilling Needed to Prepare Workforces. (2025, Jan).

the risks.[261] This principle is directly transferable to defence: interdisciplinary collaboration, between engineers, commanders, legal advisors, ethicists, and strategists, is essential to building AI and Cyber capabilities integrated forces that are not only operationally capable but also aligned with international law and humanitarian standards. An ethical, human-centred approach to military innovation will be just as important as technical mastery in shaping the armed forces of the future.

In an era defined by rapid technological convergence with AI and Cyber at the forefront, a siloed approach to capability development and governance is no longer tenable. Contemporary regulatory frameworks are beginning to reflect this shift, increasingly highlighting the necessity of broad-based AI literacy across both civilian and military domains. Notably, Article 4 of the EU Artificial Intelligence Act (EU AI Act) explicitly underscores the importance of fostering awareness and understanding of AI among a wide range of stakeholders, not just technical experts. However, the lack of a unified global regulatory framework continues to pose a strategic challenge, potentially impeding the harmonised development of norms and standards essential for cross-domain interoperability and ethical governance.

NATO has recognised the strategic importance of addressing this gap and is actively promoting an integrated understanding to AI and Cyber across the Alliance. NATO is facilitating multidimensional engagement that extends well beyond the technical sphere organizing, for example, AI Workshops across the Organization to enhance its capabilities and

[261]Future of Jobs Report 2025: 78 Million New Job Opportunities by 2030 but Urgent Upskilling Needed to Prepare Workforces. (2025, Jan). Ibid.

understanding, aligning relevant stakeholder and Allies. These initiatives intentionally encompass broader considerations, including, for example, the ethical implications of deploying autonomous weapons systems, such as Unmanned Aerial Systems (UAS) and Unmanned Aerial Vehicles (UAVs), as well as legal compliance challenges, such as third-party risk management. This reflects an institutional commitment to fostering an operational culture where technological sophistication is matched by strategic foresight and normative responsibility.

7.3 Regulatory Evolution and Guidelines

The prominent role of Cyber and AI in contemporary military strategies is increasingly reflected in a growing body of international regulations and strategic guidelines. These include the EU AI Act, the Cyber Resilience Act (CRA), NATO's AI Strategy, and the U.S. Department of Defense's Ethical Principles for Artificial Intelligence. While these instruments underscore a shared recognition of the strategic importance of these technologies, the persistent absence of a unified global regulatory framework, frequently noted in this chapter, remains a significant challenge to coherence and interoperability across allied and partner nations.

Nonetheless, the existing regulations, despite their intrinsic differences, appears to be leading towards a common objective: striking a balance between technological innovation and ethical responsibility. They aim to ensure that the development and deployment of AI systems and their Cyber implications remain aligned with IHL, while preserving essential principles such as human oversight, accountability, and meaningful

human-machine collaboration. These foundational goals are particularly significant in the military and defence context, where the implications of autonomous decision-making and the use of force demand rigorous legal, ethical, and operational scrutiny. As a result, such regulatory efforts are increasingly shaping how AI and Cyber capabilities are integrated into defence doctrines, capability development, and operational frameworks. For instance, the EU Parliament's Special Committee on Artificial Intelligence in a Digital Age (AIDA) stressed the need for ethical guidelines in defence while balancing the EU's potential lag in AI development, calling for international regulation of lethal autonomous weapons (LAWS), robust Cybersecurity measures, and global cooperation in military AI regulation.[262] Similarly, while the 2025 European Parliament briefing notes explicitly exclude military applications from the scope of the EU AI Act, they acknowledge that the Act may nonetheless influence future discussions and normative developments concerning the regulation of military AI. [263] Finally, NATO's AI Strategy highlights collaboration with other international bodies such as the EU itself and United Nations (UN) in its principles of responsible use.[264]

The EU AI Act, adopted in June 2024, represented the first binding worldwide horizontal regulation on AI. It aims to foster AI development while mitigating risks, positioning the EU as a global leader in trustworthy and democratic AI governance.[265] As previously mentioned, the Act

[262] AIDA 2024– Special Committee on Artificial Intelligence in a Digital Age. European Parliament.
[263] Defence and Artificial Intelligence. (2025, April). European Parliament. Ibid.
[264]NATO Releases Revised AI Strategy. (2024, Jul). NATO. Ibid.
[265] AI Act. (2025, Feb). European Union.

focuses solely on commercial AI, explicitly excluding military applications and national security services due to deliberate exemptions to preserve Europe's strategic autonomy, ensuring minimal restrictions on AI in defence and security. Despite this consideration, the Act retains the distinction of being the first of its kind and holds significant potential to influence defence AI policy, particularly in areas involving dual-use technologies such as drones. Its practical application and normative framework serve as a reference point for shaping future military-specific AI regulations, especially where civilian and defence technologies converge (more frequently than ever before).

Two key elements from the EU AI Act are particularly relevant when considering the development of future military-specific AI frameworks: the risk-based approach and the human-centric approach. The risk-based model adopted by the EU Parliament signals a deliberate effort to balance innovation with responsibility. It does not seek to halt technological progress; rather, it identifies specific prohibited scenarios (n. 8) where AI development should be banned due to the potential for serious harm or violations of IHL or other human rights frameworks. Beyond these prohibited uses, the approach categorizes certain applications as high-risk, permitting innovation under strict compliance and oversight, while others are subject mainly to transparency and accountability obligations, particularly regarding the end-user impact. The human-centric approach complements this by placing individuals at the core of AI governance. As emphasised in the EU's regulatory language, technological innovation should ultimately serve human needs and values, rather than undermine

them. This principle is especially relevant in the defence sector and can guide future frameworks in the sector.

The parallelism between AI and Cyber, presented so far, is also underscored by the EU regulator, which enacted the CRA almost simultaneously with the EU AI Act, signalling a coordinated effort to address the intertwined challenges of digital security and AI governance. By the timelines and scopes of these two regulatory frameworks, the EU underscores its recognition that the development of and deployment of AI systems cannot be meaningfully separated from broader concerns around digital infrastructures, data protection, and Cyber resilience. Together, the AI Act and the CRA represent a comprehensive framework designed to protect innovation and competitiveness, while simultaneously ensuring fundamental rights.

The CRA, adopted at the end of 2024, primarily focuses on ensuring the Cybersecurity of connected digital products, both hardware and software, [266] and adopts an approach comparable to that of the EU AI Act regarding defence-related systems. This shared framework invites a deeper reflection on the evolving concept of dual-use technologies. These technologies, designed for both civilian and military applications (e.g., drones) introduce new potential threats and areas of concern by blurring the traditional boundaries that have long defined the defence market. The entry of civilian actors into this space is reshaping the rules of engagement. Both the EU AI Act and the CRA recognize this shift by excluding exclusively military applications from their scope, while explicitly encompassing dual-use

[266] Cyber Resilience Act. (2025, Mar). European Commission.

technologies, thereby addressing the unique challenges posed by their dual nature.

The US DoD has also taken significant steps to establish ethical principles for AI use and Cyber measures in defence. For instance, the DoD's Ethical Principles for AI, released in 2020, outline five key tenets: responsibility, equitability, traceability, reliability, and governability.[267] These principles guide the development, deployment, and use of AI technologies in military applications, ensuring that AI systems are used responsibly and ethically. The DoD's approach emphasises the importance of human oversight and accountability, recognising that AI systems must operate within the bounds of international law and ethical standards.[268] In 2023, the DoD also developed a comprehensive Data, Analytics, and AI strategy, focusing on integrating AI across ISR, logistics, Cyber operations, and autonomous systems.[269] The strategy includes initiatives such as the Joint Artificial Intelligence Center (JAIC) and the Defense Advanced Research Projects Agency (DARPA), which are tasked with advancing AI capabilities through their research mandates and ensuring their ethical use in defence. The DoD's approach highlights the need for robust governance frameworks to address ethical concerns and mitigate risks, ensuring that AI and Cyber measures and strategies are designed to enhance military capabilities while safeguarding human rights and IHL.

In addition to the EU and US regulatory frameworks, other international organisations are actively working to establish guidelines and standards for

[267] DOD Adopts Ethical Principles for Artificial Intelligence. (2020, Feb). US Department of Defense.
[268] DOD Adopts Ethical Principles for Artificial Intelligence. (2020, Feb). op. cit.
[269] DOD Releases AI Adoption Strategy. (2023, Nov). US Department of Defense.

AI and Cyber Governance. The Organisation for Economic Co-operation and Development (OECD) has developed AI Principles that emphasise human-centric AI, transparency, accountability, and robustness.[270] These principles serve as a framework for governments and organisations to align their AI practices with ethical standards and societal values, while also valuing Cybersecurity concerns (e.g., robustness). The OECD's approach represents an important first step toward bringing greater coherence to the competitive geopolitical landscape outlined earlier in this chapter. It underscores the need for international cooperation in establishing unified regulatory frameworks that promote the responsible development and use of AI, a widely endorsed principle that, in practice, remains difficult to implement due to prevailing national interests and the pursuit of competitive advantage. Similarly, the UN has also been involved in discussions on AI governance, particularly in the context of lethal autonomous weapons systems (LAWS).[271] The UN Convention on Certain Conventional Weapons (CCW) has hosted discussions on LAWS since 2014, with member states and non-governmental organisations advocating for a pre-emptive ban on such systems due to ethical concerns.[272] However, achieving consensus has been challenging, as some countries oppose outright bans, instead favouring regulation or codes of conduct. The UN's efforts further reinforce the challenges highlighted in the OECD context, with nations still struggling to set aside national interests in pursuit of a

[270] AI Principles. Organization for Economic Co-operation and Development.
[271] Defence and Artificial Intelligence. (2025, April). European Parliament.
[272] The Convention on Certain Conventional Weapons. United Nations.

shared global consensus on AI governance and Cyber measures, particularly when it comes to security and defence matters.

7.4 Threats, Vulnerabilities, and Mitigations

7.4.1 Threat Landscape and Systemic Vulnerabilities

The geopolitical complexity surrounding AI and Cyber matters translates into a threat landscape containing sophisticated actors and advanced exploitative mechanisms. According to the 2025 European Parliament report on Defence & AI,[273] it is outlined that state actors, such as Russia and China, despite having their weakness points still possess significant Cyber warfare capabilities, including AI-powered solutions, focusing on espionage, disruption of critical infrastructure, and influence operations. Deloitte's March 2025 Global Cyber Threat Intelligence Report adds a further layer to the panorama identifying non-state entities, including organised crime groups, Cybercriminals, and hacktivist collectives. These, leveraging the anonymity and reach provided by Cyberspace, carry out disruptive activities ranging from financial theft to ideological sabotage.[274] State actors typically engage in advanced persistent threats, which may include prolonged efforts to infiltrate and exfiltrate sensitive data from strategic targets. As such, state actor capabilities include multi-vector attacks, combining Cyber intrusion with psychological and kinetic operations to achieve strategic objectives. On the other hand, non-state actors, which are typically less resourced, have nonetheless developed sophisticated tactics that can cause significant disruption at relatively low

[273] Defence and Artificial Intelligence. (2025, April). European Parliament.
[274] Global Cyberthreat Intelligence. (2025, March). Deloitte.

cost. One example includes Cyber mercenaries who offer their malicious capabilities as services to the highest bidder, thereby augmenting the threat landscape with highly skilled adversaries.

A leitmotiv of this chapter, Cyber threats are being exacerbated by the rise of AI-powered malicious capabilities proving as a new and evolving challenge for NATO and its partner countries. Machine learning algorithms and AI frameworks automate and optimise Cyber-attacks making them more efficient and harder to detect. Some examples of this would include malware that can adapt and evolve in response to Cybersecurity measures, AI-driven spear phishing campaigns that increase success rates, seem more human, and automate exploitation of vulnerabilities.[275] Insurgent groups and rogue states can harness AI's predictive capabilities to anticipate and thwart defence mechanisms, posing a significant challenge to NATO and its partners.

Indeed, the growing exploitation of AI in Cyber threats introduces unique and unprecedented dimensions that must be considered when analysing the evolving threat landscape. Such considerations are, for example, integrated into the Cyber & AI Risk Assessment approach developed by Deloitte Italy's Data & AI Ethics service line.[276] Drawing on regulations and best practices, the methodology underscores that, when applied to the domain of AI, Cybersecurity primarily focuses on protecting AI systems themselves from Cyber threats. This includes vulnerabilities such as input injection, where malicious data is intentionally fed into AI models to alter their behaviour, and data poisoning, which targets the training datasets to

[275] Defence and Artificial Intelligence. (2025, April). European Parliament, op. cit

[276] Deloitte Data Ethics & AI Internal Sources – Cyber & AI Risk Assessment.

embed vulnerabilities or biases into the model. Model poisoning, instead, refers more specifically to the direct manipulation of an AI model's parameters with the intent to degrade its performance.

The methodology developed by Deloitte Italy's Data & AI Ethics highlights that another critical vulnerability lies within the digital supply chain fragility. The interconnected nature of modern supply chains means that Cybersecurity weaknesses in one segment can propagate through the entire network, opening numerous points of entry for Cyber adversaries. The integration of third-party components and services, often sourced globally, heightens the risk of supply chain attacks. These attacks exploit trust relationships to insert counterfeit hardware or malicious software, bypassing traditional security measures and allowing attackers to compromise systems with relative ease. Furthermore, according to the 2025 European Parliament report, [277] AI's nature as a dual-use technology further expands the threat landscape. Although originally designed for civilian purposes, these technologies can be readily adapted for military applications, increasing the risks of surveillance, communication disruption, and manipulation of systems critical to national security. Compounding this challenge is the proliferation of IoT devices, many of which are inadequately secured and easily accessible, providing adversaries with new attack vectors that can be exploited to cause widespread disruption.

Finally, insider threats, although a more traditional area, remain a perennial concern, particularly as adversaries can recruit or coerce individuals within

[277] Defence and Artificial Intelligence. (2025, April). European Parliament, op. cit.

organisations to facilitate Cyber-attacks. These insiders often have legitimate access to internal networks and data, making it easier to bypass external security measures. The combination of inside knowledge with external Cyber capabilities can lead to devastating breaches, compromising sensitive information and operational integrity, as well as public trust in institutions like NATO.

Given the expanding and increasingly complex Cyber-AI threat landscape, it is essential to develop and implement robust mitigation strategies. These strategies must transcend traditional Cybersecurity frameworks, building upon established principles while adapting and, when necessary, fundamentally transforming them to address the unique challenges introduced by AI. In this context, NATO and its partners deploy a variety of countermeasures aimed at strengthening Cyber AI resilience and enhancing defence capabilities to effectively respond to the evolving threat environment.

7.4.2 Cyber-AI Threat Mitigation Strategies

At the forefront of the mitigation efforts deployed by NATO to face the Cyber AI threats introduced above, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) supports exercises including NATO's annual Cyber Coalition Exercise. This is among the largest collective Cybersecurity efforts aimed at enhancing the Alliance's Cyber defence capabilities and interoperability among member and partner nations.[278] It focuses on improving coordination, information sharing, and collective response through simulated scenarios and collaborative training that test

[278] Cyber Coalition: NATO's Flagship Cyber Exercise. NATO.

the preparedness and response capabilities of member states. The role of AI, both as an opportunity and a potential new threat, has been deeply analysed in recent editions. Furthermore, these types of exercises serve as an opportunity to enhance training and education capabilities, essentials for developing a cadre of skilled Cybersecurity professionals within the NATO ecosystem able to mitigate the risks posed by the previously introduced threats. Other examples of notable initiatives include the NATO Cyber Range and projects from the NATO CCDCOE and the NATO Communications and Information Academy (NCI) who both play a crucial role in this endeavour. In particular, these institutions offer specialised courses and practical training that cover a spectrum of Cyber defence topics, from technical skills to strategic decision-making, again with growing attention to AI related threats.

Additionally, NATO's approach to Cyber AI threat mitigation strategies extends to the enhancement of information sharing mechanisms. Platforms such as the NATO Malware Information Sharing Platform (MISP) enable rapid exchange of indicators of compromise among Alliance Cyber defenders, strengthening the overall defence posture.[279] Furthermore, the establishment of Memorandums of Understanding (MOUs) with national Cyber defence authorities make it possible to define precise mechanisms for sharing Cyber defence-related information and assistance, thereby improving incident prevention and resilience.[280] Finally, NATO's Cyber Security Centre (NCSC), based at the Supreme Headquarters Allied Powers Europe (SHAPE), epitomises centralised Cyber defence, providing

[279] Cyber Defence. (2024, July). NATO OTAN.
[280] NATO 2019 reserve organisations renew Memorandum of Understanding.

round-the-clock support to protect NATO's networks.[281] The structure, measures, and tools presented offer only a glimpse into NATO's Cyber AI defence posture and its approach to mitigating the increasingly sophisticated threats posed by both state and non-state actors. Through these comprehensive strategies, NATO aims at safeguarding its networks, enhances operational effectiveness, and protects the critical infrastructure vital to the security of its member states and the Alliance as a whole.

Beyond NATO's mitigation efforts, the aforementioned Cyber & AI Risk Assessment methodology developed by Deloitte Italy's Data & AI Ethics service line offers a comprehensive overview of Cyber AI threat mitigation models.[282] Three primary approaches emerge from this framework: proactive defence, advanced threat intelligence platforms, and robust resilience models. First, proactive defence focuses on continuous monitoring and analysis of network traffic to detect and neutralize threats before they inflict significant damage. Second, advanced threat intelligence platforms, boosted by AI and machine learning, facilitate the prediction of potential attacks and the identification of malicious behaviour through analysis of patterns and historical data, providing real-time insights essential for pre-emptive action. Finally, robust resilience models play a crucial role in ensuring that systems can endure and swiftly recover from cyberattacks. These models incorporate the principles of redundancy, decentralisation, and sustainability. Redundancy ensures that critical functions do not rely on a single point of failure, decentralisation

[281] NCIA | NATO Cyber Security Centre.
[282] Deloitte Data Ethics & AI Internal Sources – Cyber & AI Risk Assessment.

distributes resources and capabilities across multiple locations, and sustainability focuses on maintaining long-term operational effectiveness. Starting from this theoretical foundation, the methodology developed by Deloitte Italy's Data & AI Ethics service line identifies three key elements essential to any Cyber AI mitigation effort: process, scope of application, and framework. This ensures that Cyber-AI threats are systematically identified and managed. Building on these key elements, the approach further outlines a process for handling potential Cyber AI risks, offering a practical example of how mitigation efforts can be structured, including the following phases: context analysis, risk identification, assessment, evaluation, treatment, and continuous monitoring. The context analysis phase establishes a clear understanding of the organisation's internal and external environment, enabling timely risk identification. Next, the identification phase focuses on pinpointing critical assets, potential threats, and existing controls. The assessment phase defines evaluation criteria, thresholds, and organisational risk appetite to measure the inherent risks associated with these assets. This is followed by an evaluation of control effectiveness and calculation of residual risks, which together shape the organisation's overall AI cybersecurity posture. Progressing, the treatment phase involves selecting appropriate risk mitigation strategies such as risk transfer, avoidance, or acceptance. Finally, the monitoring phase ensures ongoing risk management through the use of Key Risk Indicators (KRIs).

In conclusion, beyond Deloitte's contribution as an illustrative approach, several fundamental practices for managing cyber risks remain valid, even as AI increasingly reshapes the threat landscape. Key among these are strong cyber hygiene measures, such as regular system updates, patch

management, and user education, which are essential to minimizing the risk of vulnerabilities being exploited. Equally important are robust incident response protocols that provide a structured and effective framework for managing cyber incidents. These protocols establish clear incident reporting procedures, define specific roles and responsibilities, and outline predefined actions based on the severity and nature of each incident, ensuring a timely and coordinated response.

7.4.3 Cyber as a Strategic Enabler

AI and Cyber technologies not only have the potential to generate threats but standing as complementary pillars in modern defence strategy can be the source of relevant opportunities, particularly within MDO.[283] These technologies are, indeed, instrumental in achieving operational effectiveness and decision superiority, key concepts that define contemporary conflict scenarios.

AI's ability to process vast amounts of data and provide actionable intelligence in real time significantly enhances situational awareness.[284] Indeed, machine learning models analyse historical data to identify patterns and predict future adversary actions, allowing for proactive measures rather than reactive responses. This predictive capability provides a strategic advantage, enabling NATO forces to anticipate and counter threats effectively, making informed decisions swiftly, a critical factor in dynamic operational environments.

[283] Trustworthiness for AI in Defence. (2025, May). European Defence Agency, op. cit.
[284] Defence and Artificial Intelligence. (2025, April). European Parliament, op. cit.

Complementary, cyber capabilities bolster this effectiveness by ensuring secure communications, reliable data exchange, and protection against electronic warfare. The integration of Cyber defences within MDO ensures that operations across land, sea, air, space, and Cyber domains are cohesive and resilient. Cyber and AI technologies, in fact, provide the backbone for command-and-control structures, enabling seamless coordination and execution of complex missions. Further, Cyber technologies also ensure the integrity and security of critical infrastructure. This includes safeguarding power grids, communication networks, and transportation systems from Cyber-attacks, ensuring that logistical and operational support remains uninterrupted. The ability to defend these assets is crucial for sustaining long-term military operations and maintaining societal stability.

In essence, AI and Cyber capabilities embody the principles of modern warfare: speed, agility, and precision.[285] They have the potential to empower NATO forces to operate with a high degree of operational effectiveness, ensuring that decision superiority is maintained. As NATO continues to evolve its strategic framework, the integration of AI and Cyber technologies will only grow in importance, solidifying their role as enablers of the Alliance's defence and deterrence capabilities. The deployment of AI and Cyber technologies extends beyond immediate tactical advantages and strategic and logistical concerns. It represents a day-to-day opportunity across all type of combat scenario.

[285] DOD Releases AI Adoption Strategy. (2023, Nov). US Department of Defense, op. cit.

In the battlefield, for examples, AI-powered systems such as autonomous drones and unmanned ground vehicles can conduct reconnaissance, deliver supplies, or provide critical support to troops without exposing human assets to unnecessary risks. These systems are equipped with advanced sensors and communication tools, ensuring that real-time data can be gathered and disseminated to command centres swiftly. In the air, AI-enhanced systems assist pilots in identifying threats, navigating complex environments, and maintaining optimal flight paths. Algorithms can assess aircraft performance and predict maintenance needs before any issues manifest, thus improving operational readiness and reducing downtime.[286] AI-based threat detection systems can also identify and neutralize incoming missiles more effectively than manual systems, enhancing aerial defence capabilities. For naval operations, AI and Cyber technologies provide robust methods for monitoring vast maritime environments. Autonomous submarines and surface vessels can patrol critical waters, detect anomalies, and gather intelligence on enemy movements. AI-driven predictive maintenance allows naval forces to manage a fleet more effectively, ensuring that vessels remain combat-ready without unexpected failures. Secure communication networks enabled by advanced Cyber technologies are essential for coordinating operations between ships and integrating naval activities with land and air forces.

Space is the final frontier where AI and Cyber technologies play crucial roles.[287] Satellites equipped with AI-powered sensors can detect and track

[286] Waqas A., Artificial Intelligence in Aviation: A Review of Machine Learning and Deep Learning Applications for Enhanced Safety and Security. (2025, Feb). Premier Journal of Artificial Intelligence.

[287] EU Space Strategy for Security and Defence. (2023, Nov). European Parliament.

objects, gather intelligence, and facilitate secure communication channels across various domains. Space-based surveillance systems provide unparalleled situational awareness, allowing NATO to monitor vast areas and respond quickly to emerging threats. Cyber defence mechanisms protect these satellites from space-based Cyber-attacks, ensuring that their functionality and reliability are maintained.

Concluding, Cyber and AI technologies serve as critical strategic enablers within the framework of MDO. By enhancing situational awareness, ensuring secure and resilient communications, and enabling rapid, data-driven decision-making, these technologies unify efforts across land, sea, air, space, and cyber domains. Their integration supports operational effectiveness and decision superiority, which are vital for maintaining an advantage in today's complex and dynamic conflict environments. As stated above, being a foundational pillar of modern defence, Cyber and AI capabilities have the potential to facilitate across NATO seamless coordination, strengthen defence postures, and contribute to the sustained readiness and resilience of allied forces but solely if applied responsibly and in line with the defined PRUs.

Understanding the evolving threat landscape, along with the complexities and opportunities presented by integrating AI and Cyber systems, underscores the need for continuous adaptation and innovation, especially within the defence sector. This dynamic environment demands a balanced approach that combines technological advancement with strong risk management, AI literacy, and awareness, ensuring that both the benefits and risks of AI and Cyber integration are effectively understood and

managed while protecting against emerging vulnerabilities and operational challenges.

7.5 Strategic Recommendations

Moving towards the end of this contribution, as the convergence of AI and Cyber capabilities reshapes global security dynamics, NATO and its partner countries face an urgent challenge: to govern emerging technologies responsibly while maintaining a decisive strategic edge. The integration of AI into defence and Cyber operations brings both unprecedent opportunities and complex risks, demanding coordinated action across governance, capability development, strategic planning, and institutional awareness. This final section outlines and details four key strategic priorities to address this evolving landscape. First, it calls for robust cyber risk governance and AI-aligned frameworks for partner countries. Second, it emphasizes the need to scale NATO's AI-driven capabilities, leveraging innovation hubs and autonomous defence architectures. Third, it highlights the importance of strategic simulation and scenario-based planning to anticipate threats and stress-test responses in increasingly contested digital domains. Finally, it underscores the foundational role of digital fluency and strategic awareness, ensuring that leadership and institutions are well equipped to navigate the ethical, legal, and geopolitical challenges of the AI-Cyber nexus.

7.5.1 Cyber Risk Governance and AI-Aligned Frameworks for Partner Countries

To ensure alignment and resilience across the Alliance, partner countries must adopt interoperable cyber risk governance frameworks that embed

AI-specific risk management, accountability, and ethical safeguards into national and joint defence architectures. Drawing on instruments such as the NATO PRUs, the EU AI Act and CRA, these governance frameworks have the potential of providing clear regulatory baselines, promote secure and ethical by-design technologies, and enable real time risks detection and mitigation, as well as unifying NATO's operations across the Alliance.

In order to do so, NATO need not start from scratch; instead, it should adapt and modernize existing principles, procedures, and frameworks to align with the current geopolitical and technological landscape. Indeed, an effective cyber risk governance framework must be based and incorporate trusted, real-time cyber threat intelligence sharing among Allies and partners, stressing the collaborative nature already presented in the mitigation strategies. By leveraging secured federated learning architectures and building on NATO's Cyber Threat Intelligence Framework, for example, participating countries can strengthen collective detection and response capabilities. In addition, the establishment and strengthening of AI-enabled fusion centres would facilitate the rapid correlation of threat patterns as well as fostering the modernization of current frameworks with the integration of AI issues and considerations.

The US DOD's Data, Analytics, and Artificial Intelligence Adoption Strategy provides an example of a foundational model for cyber risk governance and AI-aligned frameworks that could serve as a reference or starting point for partner countries, supporting federated and interoperable approaches. Although not framed explicitly in terms of multinational governance, the strategy emphasises the importance of risk-adjusted, data-driven, and mission-oriented governance structures capable of operating

across diverse and complex environments.[288] Central to this approach is the recognition that effective Cyber governance must be integrated with AI assurance mechanisms, policy reform, and the removal of institutional barriers that inhabit secure information sharing. It also underscores the strategic imperative of building a robust, international AI and data ecosystem. One that advances interoperability, supports shared values, and enables trusted collaboration with allies and partners. Through the adoption of open standard architectures, shared AI services, and joint infrastructure investments, the strategy implicitly provides a blueprint for developing AI-aligned governance frameworks capable of fostering mutual resilience, accelerating innovation, and ensuring compliance with democratic norms and legal safeguards.

7.5.2 Enhancing AI-Driven Capabilities

The rapid evolution and proliferation of AI technologies represent a decisive factor in strategic competition. For NATO and its partner countries, enhancing AI-driven capabilities is not only a matter of technological innovation but of operational survivability, deterrence, and superiority. Drawing again from the U.S. DOD's AI Adoption Strategy, enhancing AI capabilities requires a deliberate shift toward iterative development, agile integration, and the responsible deployment of dual-use and mission-critical AI applications.[289]

This implies building a continuous pipeline of AI-enabled-capabilities, ranging from autonomous cyber defence agents to predictive logistics

[288] DOD Releases AI Adoption Strategy. (2023, Nov). US Department of Defense, op. cit.
[289] DOD Releases AI Adoption Strategy. (2023, Nov). US Department of Defense, op. cit.

systems, within both the tactical edge and the strategic command layers. Central to this approach is the creation of a federated innovation ecosystem where NATO's DIANA and the NATO Innovation Fund play a key role in funding, testing, and scaling solutions developed in collaboration with trusted private sector actors. To increase operational readiness, AI systems must be fielded in minimum viable configurations, validated through real-world data, and rapidly iterated via cycles of feedback between end-users and developers.[290] In order to enhance AI capabilities, it is necessary to involve designing systems that are resilient, certifiable, and adaptable to adversarial environments. For example, the European Defence Agency (EDA) recommends risk-based engineering frameworks, with modular development lifecycles and AI-specific performance metrics (e.g., explainability, autonomy, accountability, and so on) to evaluate trustworthiness under mission conditions[291].

Furthermore, harmonizing legal and operational standards for AI capabilities through shared norms, such as those outlined in NATO's Digital Transformation Implementation Strategy (DTIS) of 2022 and the Revised AI Strategy of 2024, is essential for maintaining public trust and strengthening NATO's collective AI capabilities. Allied countries currently face significant disparities in AI maturity, which create vulnerabilities within the Alliance. To address these gaps, NATO should invest in a clear, unified, and practical strategy aimed at reducing these asymmetries and enhancing the overall AI readiness and resilience of its members.

[290] DOD Releases AI Adoption Strategy. (2023, Nov). US Department of Defense, op. cit.
[291] Trustworthiness for AI in Defence. (2025, May). European Defence Agency, op. cit.

7.5.3 Strategic Simulations and Scenario-Based Planning

NATO must deepen and continue its investment in strategic simulations and scenario-based planning. These tools enable military and political leaders to explore a broad spectrum of potential futures, testing responses to complex and dynamic threats before they materialize. By incorporating and extending on AI-driven war-gaming, cyber-attack simulations, and hybrid warfare scenarios (e.g., MDO), NATO can identify vulnerabilities and assess the robustness of existing doctrines and capabilities. This proactive experimentation fosters agility and resilience, ensuring that Allied forces are not only reactive but anticipatory in the face of emerging challenges. In particular, the use of quantum computing-enhanced simulations could dramatically improve the fidelity and speed of scenario analysis, offering unprecedented strategic foresight, despite some research still needed in this direction.

Moreover, scenario-based planning facilitates cross-domain integration by bringing together experts from AI, Cyber, logistics, legal, and operational backgrounds to co-develop and test cohesive strategies in a safe environment. Such multidisciplinary collaboration breaks down traditional silos and ensures that tactical decisions align with broader strategic objectives, including ethical and legal constraints. NATO's existing frameworks like the Cyber Coalition Exercise and CCDCOE initiatives provide valuable foundations that can be expanded to encompass AI-driven threat scenarios, ensuring that all member states share a common understanding of risks and coordinated mitigation strategies. This harmonization across the alliance is critical in preventing fragmentation in

defence postures and enhancing interoperability in joint operations, as well as harnessing the full potential of the Alliance's AI and Cyber capabilities. Finally, strategic simulations serve as a continuous learning environment for both personnel and command structures, embedding lessons learned from each exercise into doctrine revisions and capability development. The iterative nature of this approach allows NATO to adapt rapidly to technological advancements and adversarial innovations, maintaining operational superiority. It also supports decision-makers in developing strategic intuition for complex, multi-domain conflict environments where AI-enabled adversaries may operate unpredictably. Scenario-based planning is not merely a preparatory tool but a strategic asset that underpins NATO's collective security architecture in an era of rapid technological change.

7.5.4 Digital Fluency and Strategic Awareness

At the end, as mentioned several times in this text, people remain at the centre. In a time where AI and machine-based software are taking the centre of the stage, NATO must continue to prioritize building digital fluency and strategic awareness across all levels of its personnel and reinforce these efforts. Digital fluency goes beyond technical proficiency to encompass a broad understanding of how emerging technologies influence strategic contexts, operational decisions, and ethical considerations. As AI and Cyber capabilities become embedded in military systems, commanders, policy makers, and operators need to comprehend not only how these tools function but also their potential implications on security dynamics and international norms. By cultivating this holistic awareness, NATO ensures that its workforce can effectively leverage

technology, mitigate risks, and make informed decisions under conditions of uncertainty and complexity.

Strategic awareness also involves embedding an ethical and legal framework within digital literacy programs to reinforce the responsible use of AI and Cyber capabilities. This includes familiarizing personnel with IHL, human rights considerations, and alliance-specific policies and principles such as the PRUs. Such integration fosters a culture of accountability and vigilance, reducing the risk of misuse or unintended consequences during operations. NATO's educational institutions, including the NATO NCI Academy and CCDCOE, play a pivotal role by offering tailored curricula that combine technical training with strategic and ethical perspectives, ensuring personnel are equipped to navigate evolving threat environments with prudence and clarity.

Furthermore, enhancing digital fluency supports interoperability and collaboration within NATO and with partner nations. A shared foundational knowledge of AI, Cybersecurity, and digital tools strengthens communication and coordination across diverse teams and operational domains. It also facilitates rapid adaptation as technologies and tactics evolve, enabling the alliance to maintain a competitive edge. By fostering continuous learning and upskilling, NATO prepares its forces not only for today's challenges but also for the unpredictable technological landscape of the future, reinforcing collective defence and deterrence in an era where digital transformation is a defining feature of global security.

In conclusion, as the convergence of AI and Cyber technologies reshapes the geopolitical and security environment, NATO faces both profound opportunities and complex challenges that demand a holistic and forward-

looking strategic approach. The alliance's ability to govern emerging technologies responsibly, while accelerating innovation and operational integration, will be pivotal to maintaining its strategic edge and collective resilience. By advancing interoperable cyber risk governance, scaling AI-driven capabilities, investing in rigorous strategic simulations, and fostering comprehensive digital fluency, NATO can navigate the uncertainties of the AI-Cyber nexus with agility and ethical clarity. These priorities collectively ensure that technological advancements serve to enhance, not undermine, the Alliance's core principles, operational effectiveness, and democratic values.

Ultimately, the human dimension remains at the heart of NATO's adaptation to this new era. Ensuring that personnel across all ranks and roles possess the strategic awareness, ethical grounding, and digital skills necessary to wield advanced technologies responsibly is essential for sustaining trust and cohesion within the Alliance. As adversaries increasingly harness AI and Cyber capabilities, NATO's steadfast commitment to continuous learning, multidisciplinary collaboration, shared norms, and a human-centred approach will be the defining factors that distinguish the Alliance in an ever more contested and complex global landscape.

Chapter 8 — Space Domain

Space is the domain that makes all other domains possible. Without PNT services, land forces cannot coordinate fires with precision. Without SATCOMs, maritime task groups lose command and control as soon as terrestrial networks fail. Without space-based ISR, the fused operational picture that MDO requires cannot be assembled. Space does not generate effects that are directly visible on the battlefield — it enables the effects of every other domain, silently and continuously, until it is denied.

That dependency has become a strategic vulnerability. The February 2022 cyberattack on the ViaSat KA-SAT satellite network — executed in the hours before Russian ground forces crossed the Ukrainian border — degraded Ukrainian military communications precisely because they relied on space-based infrastructure that was insufficiently protected and had no resilient alternative. The subsequent improvised provision of Starlink terminals to Ukrainian forces by the United States demonstrated both the operational value of commercial space access and the fragility of relying on it: a private company's pricing and connectivity decisions became, for a period, a variable in a sovereign nation's defence. These episodes did not simply illustrate the importance of space in modern conflict. They illustrated the institutional gaps — in governance, in resilience planning, in the capacity to absorb and sustain space-based capabilities independently — that SFA in the space domain is designed to address.

The contribution that follows examines how NATO and its Allies are beginning to build the frameworks, programmes, and advisory structures

that space SFA requires. The Regional Space Advisor Program of the United States Space Force — which deploys trained Guardians to geographic combatant commands and diplomatic missions to advise on space integration and foster regional partnerships — represents the most institutionally developed example of space-focused SFA currently in operation. It demonstrates that space SFA is not a theoretical construct but an operational reality that is already being professionalised, with dedicated career pathways, certified training, and governance structures designed for sustained multi-year engagement.

What this chapter adds is the analytical framework which allows that experience to be generalised. Building on lessons drawn from past SFA campaigns — including the persistent challenges of advisor selection, host-nation ownership, end-use monitoring, and interagency coordination that proved decisive in Iraq and Afghanistan — the chapter proposes a sequenced adaptation of the assess, generate, organize, train, enable, advice, mentor model tailored to the unique technical, legal, and strategic characteristics of the space domain. Space advisors must navigate export control regimes, data classification requirements, dual-use technology constraints, and attribution complexities that have no equivalent in land-based SFA. The framework developed in this chapter accounts for these specificities rather than importing land domain assumptions into a fundamentally different operational environment.

The implications for this paper's central argument are direct. Partner forces that cannot access, sustain, or protect space-based services — PNT, communications, ISR — are not simply less capable in the space domain. They are structurally dependent on external provision for the functions that

make their operations in every other domain coherent. SFA in the space domain is not, therefore, a specialised addendum to the Alliance's assistance architecture. It is a precondition for the kind of institutional resilience that MDO demands.

Space Domain Considerations

Dr. Francesca Bajardi (ITA), Author

NATO Security Force Assistance Centre of Excellence (NATO SFA COE), Former Researcher

NATO Space Centre of Excellence (Space COE), Reviewer

8.1 Introduction

Space was officially recognised as NATO's fifth operational domain in December 2019 during the Leaders' meeting in London.[292] This notable move reflected a broader international shift towards space as a critical domain of operations. In fact, on 20 December 2019, the United States established the U.S. Space Force (USSF), signalling the growing perception of space as a national security imperative.[293] In the same year, the Allies adopted the NATO Space Policy "to guide the support provided by the Allies to operations in areas like communications and intelligence".[294]

8.2 NATO's Space Infrastructure

Building on this strategic foundation, NATO began reinforcing its institutional presence in space. On 22 October 2020, NATO's Defence Ministers agreed to set up a Space Centre at Allied Air Command in

[292]NATO 2019, NATO's Overarching Space Policy. Brussels: North Atlantic Treaty Organization.
[293] United States Space Force. About Us. Washington, DC: United States Space Force.
[294] NATO 2019, NATO's Approach to Space. Brussels: North Atlantic Treaty Organization.

Ramstein[295], Germany. This centre plays an important role in defence and deterrence capabilities by facilitating the exchange of information on potential threats, managed by a dedicated multinational team. Its function is not limited to supporting operational headquarters but extends to assisting tactical units as well,[296] while also serving as a central hub for enabling NATO's activities, operations, and missions in the space domain, promoting information sharing and helping to coordinate the contributions of Allied nations.[297] These efforts contribute to NATO's core tasks, including collective defence, crisis response, and counterterrorism.[298] Building on these milestones, NATO has continued to strengthen its institutional approach to the space domain.

Parallel to these institutional developments, several NATO member states have also established dedicated national space commands, such as those of the United Kingdom, France, Germany, and Italy, highlighting the strategic relevance of space in their defence policies. Turkey, likewise, is advancing toward the creation of its own space command, aiming to enhance national capacities in areas like PNT, space situational awareness (SSA), meteorological and oceanographic data (METOC), in alignment with its broader space strategy. This growing national investment in the domain contributes to Alliance-wide interoperability and collective readiness.

A further effort to centralise expertise and enhance interoperability is the establishment of the NATO Space Centre of Excellence (COE) in Toulouse, France. This initiative reflects the Alliance's growing

[295] Supreme Headquarters Allied Powers Europe NATO Space Centre
[296] NATO Rapid Deployable Corps Italy (NRDC-ITA). NATO Space Centre.
[297]NATO 2019, NATO's Overarching Space Policy, op. cit.
[298] NATO Allied Command Transformation, NATO's Approach to Space

recognition of the strategic importance of space and its commitment to enhancing space-related capabilities.[299] In January 2023, fifteen Sponsoring Nations[300] signed the Operational Memorandum of Understanding, formalising their support for the Centre. Subsequently, on 14 July 2023, during the NATO Summit in Vilnius, the NATO Space COE received official accreditation. Once fully operational, the Centre will serve as a key driver in the development and integration of space power, offering tailored expertise and practical solutions to benefit NATO and its member states, while supporting the role of the Space Centre at Allied Air Command in Ramstein.[301]

In 2024, NATO further expanded its space architecture with the creation of the Combined Force Space Component Command (CFSpCC) [302] and the NATO Space Operations Centre (NSpOC),[303] both located at Ramstein.[304] These new bodies significantly enhance the Alliance's ability to coordinate and conduct space activities alongside operations in the traditional domains of land, sea, air, and cyber.

These institutional and national developments take place against the backdrop of a rapidly evolving space landscape. Today, access to and use of space capabilities are no longer limited to a few technologically

[299] NATO Allied Command Transformation, Space: NATO's Newest Centre of Excellence

[300] Belgium, Czech Republic, France, Germany, Greece, Italy, Luxembourg, Netherlands, North Macedonia, Poland, Portugal, Romania, Spain, Turkey, United Kingdom.

[301] Space Centre of Excellence About Space CoE. Toulouse: Space Centre of Excellence.

[302] NATO 2025, Allied Command Operations, NATO Space Domain: A New Frontier of Security. Mons: Allied Command Operations.

[303] "Currently, experts from 16 Allied Nations are assigned to the Space Operations Centre."

[304] NATO Allied Command Operations. We Coordinate NATO Space Matters. Mons: Allied Command Operations.

advanced countries; space technology and services have become more available, less expensive, and more efficient.[305] As a result, space capabilities now play an increasingly important role across a wide range of sectors. They offer significant support in civilian areas such as weather monitoring, environmental protection, agriculture, transportation, scientific research, and banking. Just as importantly, they are essential to national security and military operations, as they support and enable other operational domains by providing critical services such as communications, intelligence, surveillance, navigation, and timing, all of which are indispensable for effective MDO.[306]

In fact, thanks to space capabilities, it is possible to detect missile launches, particularly ballistic missile launches, through dedicated early warning and infra-red surveillance satellites, thus providing timely warnings and supporting defensive responses.

Most[307] of the satellites orbiting the Earth belong to NATO countries or to companies located within their territories, underlining the strategic relevance of space infrastructure for the Alliance and its strong reliance on both governmental and commercial space assets.[308]

[305] NATO 2019, NATO's Overarching Space Policy. Brussels: North Atlantic Treaty Organization, point 1.
[306] NATO 2019, NATO's Overarching Space Policy, op. cit.
[307] Around 3,000 active satellites orbiting the Earth.
[308] NATO 2019, NATO's Overarching Space Policy, op. cit.

8.3 Emerging Threats and Challenges in the Space Domain

However, this growing reliance on space also brings new challenges. The evolution of this domain has led to a certain dependency, which triggers the emergence of threats and vulnerabilities, clearly showing that space capabilities can be challenged by a potential adversary. Countries like China[309] and Russia have started developing counter-space technologies that could be able to restrict the use of space assets.[310] A clear example came in November 2021, when NATO Allies condemned Russia for conducting a reckless and irresponsible anti-satellite missile test on the 15th of that month. The test produced a large debris field in orbit, increasing the risk to human space flight and threatening the space infrastructure of many nations and organizations. In light of these developments, NATO Allies expressed their concerns regarding the increase of threats in space in the NATO's 2022 Strategic Concept.[311]

The 1967 Outer Space Treaty established space as a realm for peaceful use,[312] and militaries have relied on space since the Sputnik era primarily for security purposes. NATO and its member states recognize space as an indispensable domain to operate in, especially in crisis scenarios where terrestrial logistics are unavailable. Given this, adversaries are likely to identify and target space systems as high-value assets.

---

[309] NATO 2022, Strategic Concept, page 5, point 13,
[310] NATO 2022, Strategic Concept, page 5, point 16.
[311] NATO 2022, Strategic Concept, pag.3, point 7.
[312] 'Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies', United Nations Office for Outer Space Affairs.

In this context, threats to the space domain manifest in various forms and degrees of intensity. These range from reversible, non-destructive actions - such as jamming or interfering with communication and navigation signals - that cause temporary disruptions, to non-reversible attacks that may result in permanent damage, such as attacks by a kinetic anti-satellite weapon. Of particular concern are those actions that produce space debris, which compromise the long-term safety, accessibility and sustainability of the orbital environment. Importantly, not only space-based assets like satellites, but also ground-based infrastructure, including launch sites and control stations, as well as the links connecting these elements, are potential targets. Furthermore, space systems remain vulnerable to natural hazards and accidental failures, which can be equally disruptive and difficult to anticipate.[313]

Physical, kinetic attacks attempt to directly damage satellites, either through direct strikes, warhead detonations nearby, or by disabling key ground facilities. These weapons, commonly referred to as anti-satellite (ASAT) systems, come in different forms:

Direct Ascent Anti-Satellite (DA-ASAT) weapons, tested by China since 2007[314] and Russia as recently as 2021,[315] pose a severe threat due to the debris clouds they generate, which increase the risk of future collisions in orbit.

Co-Orbital ASATs offer a subtler threat; they operate by manoeuvring close to target satellites and are capable of causing effects from disruption

[313] NATO Space Policy, point 3.
[314] BBC News, 2007, China confirms satellite downed.
[315] NATO 2021, Statement by the North Atlantic Council on the recent anti-satellite missile test conducted by the Russian Federation'.

to complete incapacitation, while generating minimal debris and complicating attribution of intent.

One of the most severe threats is a High-Altitude Nuclear Explosion (HANE), which could incapacitate all space assets in a specific orbit indiscriminately, including those of the attacker, and is thus viewed as a last-resort measure or as asymmetric warfare, an option for an opponent that relies less on space.

Among the non-destructive methods, electronic warfare capabilities are increasingly significant. These systems operate within the electromagnetic spectrum to interfere with or block a target's ability to provide or access space-based services and systems. While they do not cause physical destruction, they can create temporary effects that last only while the system is actively targeting. This includes tactics such as jamming and spoofing of GNSS and SATCOM signals. Spoofing - sometimes called signal hijacking - involves transmitting a fake signal that misleads a receiver into interpreting it as genuine. In addition, electronic attacks may also target space-based radar systems or disrupt the reception of RF signals by users on Earth, satellites in orbit, or ground control stations.[316] The effects of these non-kinetic disruptions are not only technical but also societal. While difficult to measure precisely, long-term interference with GNSS services, such as GPS, can have substantial social and economic consequences, particularly in areas that are already facing conflict or political instability. Everyday life and essential sectors, including transportation, logistics and emergency response, rely heavily on

[316] Clayton Swope, Kari A Bingen, Makena Young and Kendra LaFave, Space Threat Assessment 2025 (Centre for Strategic and International Studies 25 April 2025).

uninterrupted satellite navigation and communication. In aviation especially, GPS interference can pose severe risks to public safety. Several UN agencies have underscored the dangers of jamming and spoofing, warning that such disruptions threaten both air and maritime safety and security.[317]

NATO's approach to space remains primarily defensive and fully consistent with international law,[318] and the Alliance has no intention of weaponizing the domain[319] as an organization.

At the same time, while remaining within the framework of international law, offensive space capabilities provided by individual member nations might need to be considered by a NATO commander in the planning and conduct of operations.

Instead of developing its own sovereign space capabilities, the Alliance will continue to rely on the assets provided by individual member nations.[320].

8.4 The Space Domain in MDO

The space domain functions both as an independent operational area and as a vital connector that supports and enhances the other domains.[321] In particular, it plays a key role in securing and enabling the flow of information gathered through space-based assets. Satellite-collected data is

[317] Ibid.
[318] NATO Space Policy, point 5, letter c.
[319] NATO 2021, Brussels Summit Communiqué. Brussels: North Atlantic Treaty Organization.
[320] NATO Space Policy, point 5, letter f.
[321] Leonardo S.p.A multi-Domain Technologies to Address Future Operational Scenarios. Rome.

vital to all NATO activities, operations, and missions. Space capabilities are indispensable for conducting ISR, supporting missile defence, providing PNT services, and enabling tactical operations across other domains. To address evolving threats such as hypersonic and manoeuvring high-speed missiles, space-based assets are increasingly taking on roles traditionally performed by manned and unmanned aerial platforms. Modern satellite constellations offer advanced Moving Target Indication (MTI) capabilities across a wide range of targets. When combined with data from PNT systems, as well as inputs from aerial platforms - including drones, High-Altitude Pseudo-Satellites (HAPS), and low suborbital vehicles - these constellations enable real-time, dynamic analysis through the fusion of multi-source, multi-platform sensor data.[322] Moreover, space plays a fundamental role in providing commanders with situational awareness[323] and accurate assessments that enable them to make informed decisions.[324] In line with this objective, in February 2023 NATO announced the creation of the Alliance Persistent Surveillance from Space

[322] Joint Air Power Competence Centre Space Domain: A Global Vision. Kalkar: JAPCC.
[323] "Speaking at the French Air and Space Academy, General Philippe Lavigne, Supreme Allied Commander Transformation, highlighted the importance of space in enabling Multi-Domain Operations, stating that Space is key to achieving this ambitious but essential… objective. Whether for situation awareness, for the credibility of our Deterrence and Defence posture, or simply to conduct operations, continuous and secure access to space capabilities, services, and products is essential." NATO Allied Command Transformation (2023) ACT Space Activities Recap 2023.
[324]NATO 2023, Alliance Persistent Surveillance from Space (APSS).

(APSS)[325] initiative.[326] By enhancing the Alliance's ability to collect and integrate space-based surveillance and intelligence, APSS is designed to further strengthen situational awareness and support faster, more precise decisions in complex operational environments. Complementing this initiative is *Aquila*, a new project that aims to establish a large-scale, virtual constellation by linking national and commercial surveillance satellite systems.[327]

To support such ambitions, recent advancements in space technology are unlocking new opportunities. Innovations in digital engineering, along with the miniaturisation of onboard systems, are facilitating the development of more adaptable and capable satellite platforms. These include global and mega-constellations, modular and distributed space architectures, high-resolution sensors, and satellites equipped to handle significantly larger data volumes: key assets for meeting the growing

[325] "APSS is not about creating NATO-owned and operated space assets. It will make use of existing and future space assets in Allied countries and connect them together in a NATO virtual constellation called "Aquila". This is a data-centric initiative. As such, APSS will be 'sensor-agnostic and solution-agnostic"; it will be open to all existing – and future - space assets, regardless of their scope, technologies and specificities. It will bring together both government-owned and commercial space assets. APSS will also enhance how NATO is collecting, processing, exploiting and disseminating intelligence through more comprehensive cloud solutions and technologies. AI analytical tools will be key to better manage the growing amounts of data. As such, the initiative is part of NATO's ongoing digital transformation and NATO 2030 agenda".

[326] A total of 19 NATO Allies are taking part in the initiative, including Belgium, Bulgaria, Canada, Finland, France, Germany, Greece, Hungary, Italy, Luxembourg, the Netherlands, Norway, Poland, Romania, Spain, Sweden, Türkiye, the United Kingdom, and the United States.

[327] Nineteen NATO Allies are currently participating in the initiative, including Belgium, Bulgaria, Canada, Finland, France, Germany, Greece, Hungary, Italy, Luxembourg, the Netherlands, Norway, Poland, Romania, Spain, Sweden, Türkiye, the United Kingdom, and the United States.

demands of next-generation SATCOM and supporting NATO's evolving operational needs.

Building on these technological developments, the expansion of Earth Observation (EO) capabilities and the geospatial information domain is playing a pivotal role in NATO's broader digital transformation efforts aimed at achieving and maintaining information superiority. By integrating EO-derived data with inputs from a wide range of sources (including open-source intelligence), NATO is enhancing its ability to monitor the operational environment and maintain a comprehensive operational picture.[328]

Recognizing space as an operational domain shows its vital role in NATO's strategy and operations.[329] Developments like the Space Centre at Ramstein[330] and the COE in Toulouse, along with technological efforts such as APSS and *Aquila*, show that the Alliance is taking real steps to build its space skills. Most importantly, space serves as a force multiplier in MDO[331] by providing constant communication, precise targeting, and real-time intelligence. These benefits boost the effectiveness and unity of land, air, maritime, and cyber operations. NATO's growing recognition of the cross-domain nature of space is also reflected in its annual Coalition Warrior Interoperability Exercise (CWIX), described by the Alliance as its

[328] Joint Air Power Competence Centre Space Domain: A Global Vision. Kalkar.
[329] Atlantic Council 2024, NATO Multi-domain Operations: Near- and Medium-Term Priority Initiative.
[330] "Which serves as a focal point to support NATO's activities, operations and missions; share information; and help coordinate Allies' efforts in the space domain, [including] reach[ing] out to national space entities to ensure that NATO commanders have access to required space data and services." NATO (2019) NATO's Overarching Space Policy.
[331] Mondo Internazionale (2024) L'approccio spaziale della NATO tra deterrenza, resilienza e supporto operativo per la sicurezza collettiva.

premier event for testing and validating operational interoperability. In the 2023 edition, space was explicitly addressed as a key enabler of MDO, reinforcing NATO's commitment to integrating space more fully as an operational domain. Additionally, NATO's increasing reliance on both governmental and commercial satellite constellations, particularly those in Low Earth Orbit (LEO),[332] highlights a strategic move toward enhanced resilience. The widespread deployment of LEO assets is expected to strengthen NATO's space infrastructure during crisis and conflict, ensuring greater redundancy and operational continuity.[333]

8.5 Partnerships, Capacity Building, and SFA

Here, the role of SFA also comes into focus more and more. As NATO partners and Allies are strengthening their capabilities, including those in

[332] Low Earth Orbit (LEO): region of space where satellites orbit closest to Earth's surface. There is no official definition of this region, but it is usually considered to be between 160 and 1,600 km (about 100 and 1,000 miles) above Earth. Satellites do not orbit below 160 km because they are affected by atmospheric drag. (The lowest orbiting satellite, the Japanese satellite Tsubame, orbited at an altitude of 167.4 km [104 miles].) Satellites in LEO have orbital periods between 90 minutes and 2 hours. Single LEO satellites cannot generally be used for telecommunications since their constantly changing positions and fast speeds make them difficult to accurately track from the ground. To mitigate this, multiple LEO satellites can be used to create a network of linked satellites that work together to cover a large region of Earth's surface. For LEO satellites, there is a small lag time in information getting to Earth's surface. LEO satellites also cost less to put into orbit, as less energy is needed to launch them to their ultimate orbit. However, LEO satellites travel through a denser atmosphere than those at higher altitudes, and they require a more substantial power source to move at higher speeds and make any needed corrections to their low orbits. Over time these factors contribute to the deterioration of an LEO and a satellite's ability to correct its orbit, which gives a typical LEO satellite a lifespan of about 7 to 10 years.
Ken Stewart, 'Low Earth Orbit (LEO) | Definition, Distance, & Facts' (last updated 5 September 2025) Encyclopaedia Britannica. Low Earth Orbit.

[333] Atlantic Council NATO Multi-Domain Operations. Washington, DC.

space, SFA can be a factor in making partner forces interoperable,[334] technically proficient, and resilient, especially in regions where access to space capabilities is limited or developing, recognizing that no single nation can maintain space superiority alone and that cooperative frameworks are essential to ensure interoperability and collective resilience in the space domain.[335] At the same time, the Alliance's growing dependence on space assets introduces new vulnerabilities. The increases in counter-space capabilities and orbital debris underscores the urgent need to protect space as a secure, sustainable, and accessible environment. A prominent example of this approach is the United States Space Force having established the Global Partnership Directorate (S5P), which serves as the focal point for supporting and integrating Allies and partners into the evolving space enterprise. In connection with this initiative, the U.S. Space Force has also launched the Regional Space Advisor (RSA) program[336], which deploys trained space professionals - known as Guardians[337] - to advise geographic combatant commands and diplomatic missions. These advisors act as key enablers in fostering regional partnerships, aligning space capabilities with mission needs, and supporting interoperability between Allied forces[338].

[334] Wagner, E.K. (2022) 'United States Space Force and Security Force Assistance: Standing Up the Regional Space Advisor Program', SFA Quarterly.
[335] United States Space Force (2025) US Space Force Unveils International Partnership Strategy to Strengthen Space Security.
[336] Harris, K. (2023) Fact Sheet: Strengthening U.S. International Space Partnerships.
[337] United States Space Force (2022) Space Force Instruction SPFI16-116: Regional Space Advisor Program.
[338] White House (2023) Fact Sheet: Strengthening U.S. International Space Partnerships. Washington.

The RSA Program was formally institutionalized through a dedicated Space Force Instruction, which outlines its objectives, governance, and training path. A key feature is the creation of a Special Experience Identifier (SEI)[339] that recognizes service members' progression through three defined skill levels. Advancement within the program depends on the completion of academic coursework, professional internships, language proficiency, and, where applicable, joint or graduate-level education. Program oversight is distributed across USSF offices, with the Strategic Plans and Programs directorate (S5/8) acting as executive manager, while the Space Training and Readiness Command (STARCOM) is tasked with managing training.[340]

The initiative reflects a broader strategic effort, publicly highlighted between 2023 and 2024, to deepen international space cooperation and ensure that U.S. and Allied personnel are prepared to engage across military, civil, and commercial sectors in multinational contexts.[341]

A prominent recent case that illustrates key elements of space-related assistance is the United States' support to Ukraine since the onset of the Russian invasion in 2022. The U.S. has played a critical role in enabling Ukraine's access to resilient space-based services, particularly through the provision of SATCOM terminals and coordination with commercial providers like SpaceX's Starlink.[342] These capabilities have helped to

[339] US Space Force, Space Force Instruction SPFI16-116: Regional Space Advisor Program.
[340] US Space Force, Space Force Instruction SPFI16-116: Regional Space Advisor Program.
[341] Ibid.
[342] Janes (2025) Ukraine to Receive Starlink Services Under US Deal.

sustain Ukrainian command-and-control functions under conditions of electronic warfare and physical infrastructure degradation. Moreover, the United States has facilitated the delivery of commercial satellite imagery—including Synthetic Aperture Radar and electro-optical data—from private companies such as Maxar[343] and ICEYE,[344] significantly enhancing Ukraine's situational awareness and targeting capabilities. Though largely improvised in nature, these efforts highlight the potential structure and value of more formalized space SFA frameworks in future conflicts, especially in supporting resilience and operational continuity for partners facing space-denied or contested environments.

While this example underscores the value of space-enabled support in active conflict zones, it also raises broader questions about which Allied nations are equipped to provide similar assistance in other contexts.

While the United States currently leads in operationalizing space-related SFA through institutionalized programmes like the RSA, a number of Allied nations are also developing the capabilities and institutional frameworks needed to support partner forces in the space domain. France, for example, has emerged as a key European space power with a dedicated *Commandement de l'Espace,*[345] integrating SSA, military communications

[343] SpaceNews (2025) US Halts Satellite Imagery Support to Ukraine in Major Policy Shift.

[344] ICEYE (2024) ICEYE Signs Contract to Provide Government of Ukraine with Access to its SAR Satellite Constellation.

[345] The French Commandement de l'Espace (CDE) oversees military space operations through the Air Brigade of Space Operations (BAOS) and the Space Operations Command and Control Center (C3OS), which manages space situational awareness and operational activities in coordination with national agencies and allies. The Military Satellite Observation Center (CMOS) and the Military Space Object Surveillance Center (COSMOS) support satellite observation and orbital object monitoring, contributing to space protection and early warning. These structures ensure autonomous operational

(Syracuse),[346] and signals intelligence (CERES)[347] under a unified command.[348] Its doctrinal maturity and strategic outreach position France as a credible actor to conduct space-related assistance, particularly in the Francophone regions of Africa and the Sahel. Moreover, France has established bilateral space partnerships with Allies such as the United States, Germany, Italy, and the United Kingdom, while also pursuing cooperative frameworks through the EU and NATO. The *Commandement de l'Espace* is actively involved in promoting responsible space behaviour, supported by legal advisors engaged in the development and negotiation of French, European, and UN space law. These efforts culminated in France's accession to Operation Olympic Defender (OOD)[349] in October 2023 - a permanent multinational initiative led by the United States to enhance operational space cooperation.[350] This represents a major step in enabling coalition-based military space operations and demonstrates France's commitment to both sovereignty and multilateralism in space defence.

capabilities, international cooperation, and military mission support, while the Space Innovation Laboratory (LISA) fosters technological development in the space domain. French Ministry for the Armed Forces (2024) Five Years Since France Launched Space Command.

[346] French Ministry for the Armed Forces Our Space Capabilities.

[347] The French CERES satellite system represents a significant technological advancement in electromagnetic intelligence (ELINT). Comprising three low Earth orbit satellites, CERES can monitor radar and telecommunications emissions globally, day and night, under all weather conditions—even in areas inaccessible to current sensors.

[348] French Ministry for the Armed Forces (2024) Commandement de l'Espace: les enjeux de la sécurité spatiale.

[349] U.S. Space Command Multinational Force Operation Olympic Defender. Colorado Springs: U.S. Space Command.

[350] French Ministry for the Armed Forces (2024) Commandement de l'Espace: les enjeux de la sécurité spatiale.

Along similar lines, the United Kingdom has established UK Space Command[351] and maintains operational assets such as the Skynet satellite constellation,[352] while actively contributing to multinational space awareness efforts through Five Eyes[353] and NATO channels. In September 2025, UK Space Command and U.S. Space Command conducted their first joint military operation in space: a Rendezvous Proximity Operation (RPO) in which a U.S.-operated satellite inspected the UK's SKYNET 5A at geostationary orbit. This operation, carried out under the U.S.-led Operation Olympic Defender, demonstrated a high level of Allied coordination and technical precision, reinforcing the UK's role in coalition-based space security efforts[354].

These initiatives, coupled with the UK's long-standing defence engagement programmes, suggest growing readiness to engage in tailored space SFA activities. Beyond the front-line actors, countries like Canada and Germany contribute substantively to the institutional and technical

[351] UK Government UK Space Command. London: UK Government.

[352] "SKYNET is the MOD's satellite communications (SATCOM) capability, and in particular a family of military communications satellites which provide strategic communication services to the UK Armed Forces and our allies. The SKYNET 5 satellites are the most recent generation of UK military satellites. The SKYNET 6 Programme is exploiting technological advances to deliver the next generation of military communication satellites to MOD, together with the equipment and services needed to monitor, protect, control and exploit them. SKYNET 6 satellites will be complemented by commercial satellite communication services - together providing reliable, robust, agile and collaborative communication service, ensuring defence is connected globally."

[353] "The Five Eyes alliance is an intelligence network established post-World War II between the United States, the United Kingdom, Canada, Australia and New Zealand. Its genesis lies in the post-war 1946 UKUSA Agreement, intended as a cooperative arrangement for sharing signals intelligence (SIGINT). Over time, this partnership has extended its reach, becoming an integral part of global intelligence and security operations."

[354] Royal Air Force (2025) Sky is No Longer the Limit for UK-US Military Operations.

dimensions, particularly through joint SSA, satellite data sharing, and institutional capacity building within NATO frameworks.[355]



Figure 8: Joint UK–US satellite operation in geostationary orbit (Royal Air Force, "Sky Is No Longer the Limit for UK-US Military Operations", 18 September 2025)

Collectively, these Allies possess many of the technical and institutional components necessary to expand the scope of SFA into the space domain, particularly when acting within coalitions or through coordinated NATO initiatives.[356]

Figure 9 illustrates a comparative view of NATO member capabilities in key space domains—such as SATCOM, ISR, PNT, SSA, and METOC,

[355] Reuters (2025) French Military Leader Warns of Increased Hostile Activity in Space. London: Reuters.
[356] NATO 2021, 'Brussels Summit Communiqué' (14 June) para 33.

and space early warning (SEW), which helps visualize the uneven distribution of assets among Allies.[357]

	Capabilities					
Nation	SATCOM	ISR	PNT	SSA	METOC	SEW
Canada	○	○	○	○	○	
France	○	○	○	○	○	
Germany	○	○	○	○	○	
Italy	○	○	○	○	○	
Norway	○	○	○	○	○	
Spain	○	○	○	○	○	
Turkey	○	○				
UK	○	○	○	○	○	
USA	○	○	○	○	○	○

Figure 9: Space systems owned by the main space-capable NATO nations

As the chart shows, while most Allies possess core functions like SATCOM and SSA, only a few operate advanced capabilities such as SEW. This disparity reinforces the need for cooperative frameworks that pool and synchronize national assets under shared operational architectures—precisely the goal of space-focused SFA efforts.

In conclusion, while the U.S. remains uniquely positioned to conduct comprehensive space SFA missions, particularly through programmes like RSA and its close integration with commercial providers, a small group of Allies, also demonstrate the capability and strategic posture required to lead or support space SFA efforts. Their growing investments in sovereign space infrastructure, combined with established defence cooperation

[357] Joint Air Power Competence Centre Collective Defence in the Space Domain. Kalkar: JAPCC.

mechanisms, suggest a solid foundation for future missions. When structured through multilateral frameworks and aligned with NATO's overarching space strategy, these nations could effectively deliver space-related assistance across a spectrum of operational, institutional and strategic domains - helping partner forces, not only to access and utilize space capabilities, but also to become resilient, interoperable actors in an increasingly contested environment.

Maintaining safe and sustainable access to space will be critical for preserving NATO's operational edge and responding effectively to a shifting security landscape shaped by rapid technological evolution and emerging threats. Together, these programmes illustrate how tailored SFA in the space domain can serve both operational objectives and strategic cohesion among partners.

The design of effective space SFA should build upon lessons learned from past military efforts to develop and support partner forces, particularly in Iraq and Afghanistan, which revealed persistent challenges and critical success factors - even though such activities were not yet formally conceptualised as SFA. Chief among these was the need for properly selected and trained advisors: not ad hoc assignments, but centrally selected personnel with mission-specific preparation and long-term career incentives.[358] The creation of specialized formations like Security Force Assistance Brigades (SFABs)[359] significantly improved advising outcomes

[358] Mejia, D.A. et al. (2011) Improving Security Force Assistance Capability in the Army's Advise and Assist Brigade. Technical Report ADA522929.

[359] "In May 2025, the Pentagon announced plans to shutter two of the Army's six security force assistance brigades (SFABs) and to downsize Security Force Assistance Command into a small shop of about three dozen personnel within US Army Forces Command. This

by ensuring continuity and technical credibility.[360] Moreover, emphasizing host-nation ownership proved essential to avoiding dependency and aligning assistance with political end-states.[361] Conversely, inadequate equipment accountability, poor end-use monitoring, and fragmented interagency coordination undermined effectiveness and created long-term risks; such problems that are directly relevant to the space domain, where systems are sensitive, dual-use, and often commercially integrated.[362]

Translating these insights into the space domain demands a framework tailored to its unique technical, legal, and strategic characteristics. Space advisors must be equipped with a mix of skills:[363] technical expertise in satellite operations and Space Domain Awareness (SDA), cyber defence awareness, and fluency in legal regimes such as export controls and data classification. These advisor cadres must be trained through certified, domain-specific pathways, mirroring the professionalization efforts that have been initiated after oversight failures in past campaigns. Assistance should also prioritize partner ownership of SDA: not simply providing

---

decision ignores clear doctrinal and operational evidence demonstrating SFABs' strategic value—from Field Manual 3-22 accounting for the utility of Gulf War advising to how the Korean Military Advisory Group was pivotal in halting North Korea's initial assault in 1950. Yet, SFABs today face shrinking personnel authorizations and institutional ambivalence about their future". Matisek, J., Messenger, A. and Belohlavek, C. (2025) No More Train and Pray: The Consequences of Cutting the Army's Security Force Assistance Capability.

[360] U.S. Department of Defense Office of Inspector General (2022) Special Report: Lessons Learned from Security Cooperation Activities in Afghanistan.

[361] R Hooker and J Collins, Lessons Encountered: Learning from the Long War (National Defense University Press 2015).

[362] U.S. Department of Defense Office of Inspector General (2022) Special Report: Lessons Learned from Security Cooperation Activities in Afghanistan.

[363] R. Hajjar, "What lessons did we learn (or re-learn) about military advising after 9/11?" Military Review, 2014.

turnkey systems, but enabling partners to independently operate, sustain, and improve their own SSA infrastructure.[364]

To structure such assistance effectively, a sequenced framework should be adopted, adapting the traditional model. It should begin by establishing the necessary policy and governance alignment, clearly defining authorities, strategic end-states, and the roles of diplomatic, defence, civil, and commercial actors in the program.[365] Once the political and institutional foundations are in place, partners and advisors must jointly assess critical needs and risks. This means mapping dependencies on space-based services like PNT, communications, and ISR; identifying potential threat vectors and legal constraints; and evaluating the absorptive capacity and industrial maturity of the partner nation.

Following this, it is essential to design a dedicated advisory workforce.[366] These teams must integrate technical, legal, and cultural competencies and be supported by long-term institutional structures. At the same time, assistance should include modular capability packages, consisting of orbit-agnostic SDA sensors, resilient communications, ground software, and logistical support, combined with embedded training modules that facilitate autonomy and sustainability.[367]

Effective cooperation in this context also requires secure data governance. That includes implementing tiered access controls, data provenance

[364] R Hooker and J Collins, Lessons Encountered: Learning from the Long War (National Defense University Press 2015).
[365] Ibid.
[366] Mejia, D.A. et al. (2011) Improving Security Force Assistance Capability in the Army's Advise and Assist Brigade. Technical Report ADA522929.
[367] Mejia, D.A. et al. (2011) Improving Security Force Assistance Capability in the Army's Advise and Assist Brigade. Technical Report ADA522929.

mechanisms, and attribution standards that allow for trusted information sharing without compromising sensitive national information.[368] Once systems and teams are in place, advisor teams should be embedded with partner space agencies and military units to provide on-the-job mentoring and support joint exercises.[369] These activities should progressively build partner self-reliance and lead to a planned transition of responsibilities. Accountability and sustainment must also be at the core of the program. This involves applying rigorous end-use monitoring, providing maintenance and logistics training, and using performance metrics to assess sustainability and long-term impact.[370] Finally, the process should be supported by continuous feedback and adaptation. Measurable performance indicators and periodic reassessments should inform future adjustments to the assistance strategy as partner capabilities mature.[371] This framework must also take into account several domain-specific challenges that differ from traditional land-based SFA. Cybersecurity presents a critical concern. Telemetry systems, command links, and data networks used in SDA are highly sensitive and vulnerable to intrusion, requiring protection measures to be embedded into both technical systems and advisor training curricula. Attribution of responsibility for interference or hostile actions is also complex in space due to technical limitations and

[368] Reframing the Special Operations Forces-Cyber-Space Triad' (March 2024) Military Review.
[369] Reframing the Special Operations Forces-Cyber-Space Triad' (March 2024) Military Review.
[370]U.S. Department of Defense Office of Inspector General (2022) Special Report: Lessons Learned from Security Cooperation Activities in Afghanistan.
[371] R Hooker and J Collins, Lessons Encountered: Learning from the Long War (National Defense University Press 2015).

the absence of universally accepted norms. This makes deterrence and escalation control far more complicated than in traditional military domains.[372]

In practical terms, a bilateral SFA program in the space domain could start with a joint SDA pilot project, such as deploying sensors, establishing secure data links, and training analysts. This would be followed by a two-year period of embedded advising and mentorship, culminating in the full transfer of operational responsibilities to the partner nation. The program would conclude with lifecycle sustainment plans and periodic reassessment, mirroring the phased handovers used in past land campaigns.[373]

In summary, SFA in the space domain needs to be strategic, phased, and resilient. It should rest on interoperable capabilities, trained advisors, sustainable partnerships, and clear legal guidelines. By learning from past campaigns and applying proven frameworks to the space environment, NATO and its Allies can develop a network of capable, independent space partners who enhance collective security in a more contested domain.

[372] Reframing the Special Operations Forces-Cyber-Space Triad' (March 2024) Military Review.

[373]DA Mejia et al, Improving Security Force Assistance Capability in the Army's Advise and Assist Brigade (Technical Report ADA522929, US Army 2011).

Chapter 9 — Non-Military Stakeholder Interaction

The preceding chapters of this paper have examined SFA through the lens of five operational domains: land, maritime, air, space, and cyber. Each has identified the capabilities that partner forces must develop in order to contribute meaningfully to MDO, and each has identified the institutional deficits — in training, governance, doctrine, and resilience — that SFA must address. What none of the domain chapters can fully resolve is the question of which actors are required to build those capabilities, and how they must be coordinated. In the contemporary operational environment, the answer extends well beyond the military sphere. The SATCOM that sustains command and control are operated by private companies. The cybersecurity infrastructure that protects partner networks is managed by civilian agencies and commercial vendors. The governance reforms that give partner forces institutional legitimacy depend on governmental bodies, international organisations, and civil society. Synchronising these actors with military planning is not a secondary consideration: it is a structural requirement of MDO, and it is one that existing SFA doctrine has not yet fully absorbed.

This chapter addresses that gap. The contribution developed by the NATO CIMIC Centre of Excellence (CIMIC COE) introduces Civil-Military Cooperation as the doctrinal instrument through which the non-military dimension of SFA is systematically integrated into planning and execution. CIMIC, as defined in MC 411/3, is not a liaison function at the margins of military operations; it is a joint function that integrates the understanding

of civil factors across the full operating environment. In the context of SFA in MDO, this means mapping dependencies on civilian infrastructure, identifying non-military actors whose capabilities are indispensable to partner force effectiveness, and building the coordination mechanisms that allow military and non-military contributions to converge rather than conflict.

A key analytical contribution of the chapter is the distinction it draws between "human terrain" — the social, cultural, and political dynamics traditionally at the centre of SFA's civil analysis — and the full civil environment, which extends to physical infrastructure, essential services, natural resources, and the governance systems that determine whether civilian life can be sustained under the pressures of conflict and simultaneous capacity building. In NMI, this distinction is operationally consequential: advising on defence institution reform requires understanding not only the political dynamics of the Iraqi security sector but also the broader civil context — energy supply, administrative capacity, public trust — that determines whether institutional reforms can take hold and endure. Human terrain analysis alone is insufficient for that task.

The Starlink experience in Ukraine, examined in detail in this chapter, provides the most instructive recent case study of what happens when this coordination is absent. The provision of commercial SATCOMs by a private actor proved decisive to Ukrainian command and control — and simultaneously exposed a strategic vulnerability when that actor's commercial interests and policy preferences diverged from military requirements. The lesson is not that private sector involvement in military

operations is undesirable, but that it must be governed: anticipated, planned for, deconflicted, and embedded in frameworks that align objectives across actors who operate under fundamentally different incentive structures. CIMIC is the instrument NATO has for doing that work. This chapter makes the case for its systematic integration into SFA — not as an optional enhancement, but as a foundational requirement for any capacity-building effort that aspires to produce partner forces resilient enough to operate in a genuinely multi-domain environment. Practical instruments for governing multi-actor SFA delivery — stakeholder mapping, project governance, and BI safeguards in procurement — are set out in Appendix 2.

Synchronisation with Non-Military Activities: Enhancing Security Force Assistance through Civil-Military Cooperation in MDO

Lt. Col. Peter Schaefer (GS, DEU-A), Author
NATO Civil-Military Cooperation Centre of Excellence (CIMIC COE), Branch Chief

Eleonora De Martin (ITA), Reviewer
NATO Civil-Military Cooperation Centre of Excellence (CIMIC COE)

9.1 Introduction

Imagine a battlefield where the most crucial actors are no longer soldiers but satellite operators, private tech companies, and governmental organisations. In today's Multi-Domain Operations, wars are no longer fought exclusively with tanks and missiles; they are waged in cyberspace, through information networks, and within the frameworks of civil resilience. Thus, modern security challenges require not only military strength but also building resilience, fostering cross-society partnerships and synchronising efforts across all sectors. As the lines between military and civilian domains blur, the role of Civil-Military Cooperation (CIMIC) is increasingly crucial.

Particularly in the MDO framework, non-military actors play a pivotal role due to their expertise, resources, and influence over critical domains, particularly Cyber and Space. Essential infrastructure, such as satellite communications, cybersecurity networks, and supply chain logistics, is increasingly controlled by private companies. These actors not only provide capabilities that are indispensable for civil resilience but also represent potential vulnerabilities if not adequately integrated into military planning and operations. SFA activities, which aim to build the capability of partner nations to address security challenges as part of NATO's contribution to a comprehensive approach, also require synchronisation with non-military actors. These operations extend beyond traditional military training and building capabilities to include initiatives that strengthen governance, economic stability, and social cohesion[374]. As such, private sector partnerships, as well as collaboration with NGOs and development agencies, are crucial in enhancing the effectiveness of SFA activities.

This chapter will argue that synchronising with non-military actors into SFA is a strategic imperative. Military forces necessitate leveraging the civil capabilities to address modern security effectively. However, this requires robust frameworks for collaboration, clear communication channels, and mutual trust between military and non-military stakeholders. CIMIC, as a joint function, enables access to the civilian dimension of the battlespace shaping both operational freedom of action and long-term

[374] NATO 2025 AJP-3.16, Allied Joint Doctrine for Security Force Assistance, Edition B, Version 1, P.9.

stability. When fully integrated, CIMIC supports the legitimacy of operations, enhances situational understanding, and enables enduring influence in complex environments. Therefore, CIMIC needs to be systematically integrated into SFA planning and execution within MDO framework.

9.2 CIMIC: Some Definitions

According to the MC 411/3, NATO's Military Policy on CIMIC and Civil-Military Interaction, CIMIC is defined as "a military joint function that integrates the understanding of the civil factors of the operating environment, and that enables, facilitates, and conducts civil-military interaction to support the accomplishment of missions and military strategic objectives in peacetime, crisis, and conflict."[375] Furthermore, the document defines Civil-Military Interaction (CMI) as "activities between NATO entities and non-military actors aimed at fostering mutual understanding, thereby enhancing effectiveness and efficiency in crisis management and conflict prevention and resolution." These definitions underpin CIMIC within NATO, which is comprised of two primary activities: Civil Factor Integration (CFI) and CMI. The Civil Factors are described as "the non-military part of the comprehensive Operating Environment".[376]

The MC 411/3 also designated all participants in the civilian environment as non-military actors without differentiating between the civilian

[375] MC 411/3 D6 p. 5
[376] MMC 411/3 SD 5

population and humanitarian or international organisations. This approach highlights the importance of engagement regardless of the specific actors involved. *Annex A* categorises non-military actors—government/public administration, governmental organisations, private sector, international organisations, and NGOs—and outlines their respective connection with SFA. This taxonomy supports commander and staff processes by clarifying roles, likely contributions, and coordination requirements across domains, thereby enabling targeted engagement, deconfliction, and risk management.

Additionally, the policy highlights CIMIC's role in enhancing resilience, which is a vital element of Deterrence and Defence. Through the evaluation of civil preparedness, CIMIC contributes to future planning. This evaluation focuses on the three core functions of civil preparedness—continuity of government, continuity of essential services to the population, and continuity of civil support to military operations—and is primarily conducted through an extensive network of relationships.

The NATO CIMIC Doctrine, AJP 3.19, establishes the connection between policy and CIMIC implementation. As such, it clarifies the levels of interaction with non-military actors and defines CIMIC as a joint function, along with its responsibilities within the Joint Function Framework. According to the NATO doctrine AJP 01, "The joint functions framework assists commanders to integrate political, military and civil actions through the operational domains."[377] CIMIC is essential to this

[377]NATO 2022, Allied Joint Publication (AJP)-1: Allied Joint Doctrine. p. 105

framework as it coordinates military and non-military actors through its two core activities. It also facilitates the identification and analysis of stakeholders' roles and influence across various domains, enabling commanders to determine which non-military actors should be engaged and the most effective means of engagement.

9.3 CIMIC in MDO: Synchronising with Non-Military Activities

Within NATO, the evolving approach to warfare and operational planning acknowledges the necessity for a broader, effects-oriented framework that extends beyond traditional military boundaries. The concept of MDO aspires to synchronise military activities across all operational domains—maritime, land, air, space, and cyberspace— to create converging effects at the pace required by contemporary threats. However, despite this conceptual shift, the operationalisation of synchronisation with non-military activities within NATO is not yet fully defined or consistently implemented in practice.

The increasing relevance of the space and cyber domain has significant impacts on synchronisation, given the proliferation of actors—ranging from private industry and research institutions to international partners—whose capabilities are often indispensable to military operations.[378] This interdependence introduces new risks, such as competing demands for limited resources and potential vulnerabilities stemming from reliance on

[378] The Alliance's Transition to Multi-Domain Operations, An AIRCOM Perspective, Squadron Leader Shaun Cannon, UK Air Force, HQ AIRCOM

civil infrastructure. CIMIC is crucial in this context, particularly as the boundaries between military and civilian spheres become increasingly blurred in the cyber and space domains.

CIMIC's core functions—civil factor integration and civil-military interaction—are essential for aligning military planning with the realities of an increasingly complex operating environment.[379] By systematically analysing and integrating civil factors, CIMIC helps identify dependencies, capability gaps, and risks associated with civilian assets, such as private satellite networks or cybersecurity infrastructure.[380] Additionally, Civil-Military Interaction focuses on facilitating collaboration between military forces and non-military actors. This interaction is vital for ensuring access to civilian capabilities that NATO lacks but needs to operate effectively. By fostering cooperation, CIMIC can help minimise disruptions to the civil environment while optimising the use of shared resources, ensuring the military's operational effectiveness without imposing unnecessary strain on civil actors and their environment.

9.4 Challenges of Synchronisation Between Military and Non-Military Actors in SFA

Despite the increasing recognition of CIMIC, its integration with SFA remains underdeveloped due to institutional silos, divergent cultures, and limited interoperability. While MDO requires seamless synchronisation with non-military actors and cross-domain synergies, the understanding of

[379] CIMIC COE, 2025
[380] Op. cit.

the civil environment is often limited in SFA operations. This gap carries strategic consequences and implications for the effective achievement of SFA's operations goals.

One of the SFA's imperatives refers to understanding the Operational Environment. "In-depth understanding of the operational environment, including the existing FSF, current or potential threats to PN security, and especially the human terrain, is critical to planning and conducting effective SFA operation".[381] Since capability and capacity building involve long-term and complex processes, requiring the development of local forces and infrastructure,[382] the focus on Human Terrain is too narrow. Human terrain refers specifically to the social, cultural, political, and economic factors shaping the behaviour and interactions of a population—such as tribal affiliations, religious practices, or local governance structures. On the other hand, the civil environment encompasses a broader spectrum, including both societal aspects and physical elements such as infrastructure, natural resources, and the overall quality of life for civilians. For example, understanding human terrain might involve analysing local power dynamics or belief systems, whereas assessing the civil environment could include evaluating the condition of roads for troop movements, the availability of water resources, or the impact of military activities on civil infrastructure. It is essential to focus on civil factors of the operating environment because effective SFA

[381] SFA Publication, 1-10, p. 6
[382] NATO 2025, AJP-3.16, Allied Joint Doctrine for Security Force Assistance, Edition B, Version 1, A.1.

requires an integrated understanding of both human dynamics and the broader civil context.

Moreover, in the MDO Framework, coordination challenges might be even higher as the private sector, often driven by profit-seeking purposes, plays an increasingly critical role in modern conflicts. Private businesses are in control of essential elements of infrastructure and thus, they can function as an enactor and/or recipient of weaponised measures.[383] The introduction of advanced digital systems, such as satellite communications, have enabled the implementation of concepts like "network-centric warfare", where decisions are taken based on continuously updated information.[384] The positive outcome of conflicts cannot be achieved solely through military means, and survival on the battlefield requires both the military's capacity to endure on the front and the resilience of the population, as well as coordinated diplomatic, economic, and social efforts.

Ukraine's defence against the Russian war of aggression best showcases the increasing role of non-military actors and infrastructure in conflict. In 2022, the combination of missiles and cyber-attacks from Russia resulted in the shutdown of the internet within up to 25 km from the front line.[385] Targeting the communications system aimed to isolate troops and cut off the connections between soldiers and their families. To address this issue,

[383] Abels J, Bieling H-J (2023) Infrastructures of globalisation: shifts in global order and Europe's strategic choices. Competition & Change 27(3–4): 516–533.
[384] Laviniu Bojor, et al. "Emerging Technologies in Conflict: The Impact of Starlink in the Russia – Ukraine War." Revista Academiei Forţelor Terestre, vol. 29, no. 2, 1 June 2024, pp. 185–194,
[385] (Palli, 2022)

Ukraine asked for international support, both military and civilian. Among many, Elon Musk, the CEO of SpaceX and owner of the satellite constellation Starlink, responded to the call for action and restored Ukraine's communication system by providing satellite internet access in areas where traditional infrastructure and connectivity are limited.[386] Starlink rapidly became essential for Ukrainian military operations, enabling secure communications, coordinating counterattacks, drone operations, and maintaining civilian-government connectivity. However, relying on a single, privately controlled infrastructure implies new strategic vulnerabilities, as service continuity depends on Space X's decisions and interests. By mid-2022, Elon Musk questioned the company's role, sought U.S. funding, proposed a "peace plan" seen as aligned with Russian demands, and limited Starlink's use for offensive operations. This case exemplifies how the divergence between military imperatives and private sector interests can create friction, complicating the synchronisation with non-military activities.

9.5 Implications for SFA

Since 2014, NATO has provided extensive SFA to Ukraine through trust funds, advisory missions, and targeted capacity-building programs, focusing on command and control, logistics, cyber defence, and interoperability.[387]

[386] Bojor, et al., 2024, p. 188
[387] NATO 2023, NATO's support to Ukraine.

Following the 2022 invasion, NATO intensified its support, facilitating the provision of advanced weaponry, intelligence sharing, and training for Ukrainian forces, while also strengthening Ukraine's ability to withstand hybrid threats, including cyberattacks and disinformation[388]. Also, the EU has scaled its engagement through European Peace Facility, the EU Military Assistance Mission in support of Ukraine (EUMAM Ukraine), and various civilian advisory and reform programs.[389]

The case of Starlink demonstrates that building partner force capacity increasingly depends on the ability to effectively synchronise military assistance with contributions and constraints of non-military actors, including private sector providers of critical infrastructure. Failure to align objectives, timelines, and risk tolerances among these actors can undermine the sustainability and legitimacy of SFA efforts, leading to operational vulnerabilities or even strategic reversals if access to essential capabilities is curtailed.

The Starlink experience in Ukraine underscores the imperative for integrated planning and coordination mechanisms that include not only military and governmental actors but also private businesses and civil society. Overall, synchronisation with non-military actors—including humanitarian, development, and private sector stakeholders—is essential to ensure that military assistance is both effective and sustainable. This

[388] NATO 2023, Security Force Assistance.
[389] European Council. (2022). EU support to Ukraine: military assistance and training missions

aligns with NATO and EU principles of integrated crisis management and whole-of-government approaches.[390]

9.6 Bridging the Gap Between CIMIC and SFA

In light of the challenges above related to synchronisation of non-military activities, planning and implementing capacity-building activities directed to security forces requires an in-depth understanding of the Civil Factors of the Operating Environment. Identifying the key factors influencing this environment is essential for defining the goals and methods for developing local forces and institutions.[391] As geopolitical developments forced NATO to emphasise collective defence and (resilience through) civil preparedness, policymakers and military commanders need to thoroughly understand the civil environment and consider Civil Factors.

CIMIC, as a joint function, is specifically equipped to map, engage, and coordinate with such non-military actors, building trust and liaison frameworks, and manage associated risks and access constraints. It serves as a strategic integrator in this context, enabling SFA to anticipate, shape, and leverage civil factors across the operating environment. This aligns with the Remote SFA concept, which envisions a reach-back capability formed by a team of SFA Specialists who monitor mission developments, analyse regional contexts, and maintain institutional memory to ensure

[390] NATO, 2023, European Commission. (2023). EU Civilian and Military Missions and Operations.
[391] NATO 2025, AJP-3.16, Allied Joint Doctrine for Security Force Assistance, Edition B, Version 1, p. 4.

continuity across rotations.[392] SFA aims at establishing direct access to and collaborative partnerships with various entities, including national intelligence hubs, academic institutions, think tanks, and relevant international and private organizations.[393] To strengthen this effort, CIMIC can support SFA ensuring civil-military cooperation through military-military coordination.

This section aims to provide concrete domain-related examples of how to enhance CIMIC and SFA cooperation and effectively tackle challenges related to the MDO context.

9.6.1 Land Domain

SFA activities in the land domain often occur in densely populated areas where civilian governance, infrastructure, and social dynamics are critical. The land domain is not just physical, but it includes the civil actors' attitudes, networks and social structures.

CIMIC can support SFA in accessing critical civil networks, local governance structures and humanitarian mechanisms by proving not only a better understanding of the relevant non-military actors but also legitimacy.

Examples:

- **Civil Environment Assessment for training design:** CIMIC can map socio-political dynamics in the area of operations, identifying key civilian influencers, governance gaps, and

[392] NATO 2024, Security Force Assistance Centre of Excellence, REMOTE SFA, Reach Back Capability, p. 15.
[393] Ibid, p. 18.

infrastructure vulnerabilities. This supports SFA Specialists in enhancing analytical proficiency and monitoring NATO SFA campaigns.[394]

- **Sustainable partner force development:** CIMIC facilitates collaboration with local governance institutions, ensuring that partner forces are aligned with civilian authorities. For example, CIMIC can help identify legitimate civilian counterparts to work with SFA teams on long-term stabilization efforts.[395]

9.6.2 Maritime Domain

Coastal areas are populated by civilian maritime activities, from commercial vessels, humanitarian missions, fishing and tourist activities. Movement in the maritime domain should minimize the impact on civilian activities through deconfliction and coordination.

Examples:

- **Deconfliction of maritime activities:** CIMIC coordinates with port authorities, fishing cooperatives, and humanitarian organizations to ensure that SFA partner forces conducting maritime training or operations do not interfere with civilian activities.
- **Access to civilian infrastructure:** CIMIC can negotiate access to commercial docks and maritime facilities for SFA activities,

[394]Ibid. p. 14.
[395] Ibid. p. 16.

allowing partner forces to use these resources for logistical support or training exercises.

- **Building maritime awareness**: By liaising with local coastal communities and authorities, CIMIC enhances situational awareness for SFA teams, helping them train partner forces to respond effectively to threats in complex civilian-dominated maritime environments.

9.6.3 Air and Space Domains

SFA Operations also train partner national personnel via air advising and equipping them to apply air power in support of their security and governance needs.[396] An increasingly relevant domain in MDO is the Space domain. As highlighted in the examples from Ukraine, CIMIC can assist in the integration of private space actors in the SFA activities.

Examples:

- **Protocols for airspace deconfliction:** CIMIC can establish liaison with civil aviation authorities to ensure the seamless integration of SFA operations with civilians air traffic management.
- **Enhanced situational awareness through satellite data**: With many satellite systems managed by commercial or academic organizations, CIMIC can negotiate access to such

[396] Capt. Dylan A. Lenoir, (2023) 571 MSAS Air Advisors: Tactical Actors on a Strategic, SFA Quarterly 26th Ed., MAR, p. 4.

resources, improving mission planning and tactical decisions while safeguarding operational security.

9.6.4 Cyber Domain: Civilian Ownership of the Digital Battlespace

The cyber domain poses distinct challenges for SFA, as critical infrastructure, such as telecommunications, energy, finance, and data services, is predominantly owned and managed by civilian entities. This makes effective civil-military coordination vital to maintaining operational security, continuity, and societal stability. CIMIC serves as a crucial link between the military and civilian cyber ecosystem, fostering trust and establishing coordination mechanisms that enhance mutual resilience and support.

Examples:

- **Building trusted relationships with civilian cyber stakeholders**: CIMIC can facilitate liaison with Internet service providers, critical infrastructure operators, and cybersecurity agencies in partner nations. These relationships are essential for preventing cyber incidents and ensuring a rapid response to threats that could disrupt SFA activities.
- **Protecting and mitigating risks to critical infrastructure:** by analysis and assessing the civil environment, CIMIC can identify risks not only for cyber attacks but also for SFA-related cyber operations that could disrupt essential services relied upon by local populations.

9.6.5 Information and Cognitive Domains

In the modern security landscape, perception and narrative are as critical as physical effects. Adversaries target social cohesion, societal resilience and missions support through misinformation, manipulating social media with narratives to sway the local population. In the context of SFA, where building trust and legitimacy with local partners is paramount, CIMIC can assist in integrating information operations with capacity-building is essential.

Examples:

- **Aligning military messaging with local realities**: CIMIC ensures that communication efforts during SFA missions respect local cultural norms and values, enhancing the credibility of NATO and partner forces while minimizing the risk of backlash or misinformation.
- **Countering adversary disinformation:** By monitoring local media narratives and collaborating with trusted civilian stakeholders, CIMIC helps identify and mitigate the impact of adversary propaganda that could undermine SFA goals or provoke civilian unrest.
- **Supporting legitimacy and strategic communication**: CIMIC builds relationships with local journalists, influencers, and community leaders, enabling NATO and partner forces to shape the information environment in a favourable manner.

9.7 Conclusion

The complexity of the modern operational environment requires new reactive capabilities and collaboration across functions and domains. The battlespace is increasingly moving beyond the military sphere as political, informational, and societal factors become critical for operational success. Accordingly, MDO demand that SFA effectiveness hinge on NATO's ability to integrate non-kinetic dimensions—civil engagement, legitimacy building, and perception management—into capacity-building efforts.

This paper has shown that synchronisation of military and non-military activities in MDO is a strategic imperative, yet difficult to achieve given the constellation of actors and the abundance of communication pathways. CIMIC, as a joint function, provides the doctrinal, analytical, and liaison backbone to meet this challenge. By delivering a comprehensive understanding of non-military actors and the civil factors of the operating environment, mapping dependencies, and institutionalising civil-military interaction, CIMIC enables early engagement, coherent governance arrangements, and resilient access to civilian capabilities. It also supports the construction of robust liaison networks across military and non-military stakeholders to synchronise efforts, avoid duplication, and ensure that capability development is coordinated, legitimate, and sustainable.

The Starlink experience in Ukraine underscores both the decisive value and the strategic vulnerability of reliance on privately controlled critical infrastructure; access can shape outcomes, but it is neither automatic nor always aligned with military objectives. To mitigate such risks and exploit

opportunities, SFA should systematically embed CIMIC in planning, assessment, and execution across all domains—land, maritime, air, space, cyber, information, and cognitive—broadening the lens from "human terrain" to the full civil environment. Concretely, this entails: integrating civil-factor analysis into SFA design; establishing deconfliction and data-sharing mechanisms; safeguarding continuity of essential services; and aligning strategic communications with local realities.

In sum, synchronising SFA with non-military activities through CIMIC strengthens deterrence and defence, accelerates decision-making and effects in MDO, and underwrites long-term stability by aligning military objectives with the capabilities, constraints, and legitimacy of the societies in which operations unfold. Therefore, CIMIC's systematic integration into SFA is not optional—it is foundational to credible, effective, and enduring outcomes in contemporary multi-domain competition and conflict.

Annex A — Categories of Non-Military Actors

Annex A provides a practical taxonomy of non-military actors to support SFA planning and execution under the MDO framework. It defines each category and provides examples of their connection to SFA, enabling staff to map dependencies, assign liaison responsibilities, and structure engagement plans.

Category	Definition	SFA Connection
Government and Public Administration	National governments are primarily responsible for governance, security, and public services. Their agencies and public administration establish laws regulating the economy and society, ensuring the population's welfare and livelihood.	SFA is applicable only when the host nation (HN) requests assistance in developing sustainable capabilities through training and developing local forces. Commanders must integrate and coordinate NATO and HN capabilities, developing training programmes in partnership with the HN. This includes aligning training objectives, resource allocation, and responsibilities. Legitimacy of NATO and local forces in the eyes of the HN requires ongoing interaction, transparency, and cooperation.
Governmental Organisations	Entities sponsored by national governments to provide specialized support in areas such as governance, healthcare, economic development,	Governmental organisations can contribute expertise to SFA missions, especially in post-conflict reconstruction and capacity building. Their involvement in rebuilding

Category	Definition	SFA Connection
	education, and political capacity building.	infrastructure and restoring basic services supports local forces' effectiveness and stability, and their expertise can be integrated into local training programmes. **Example:** German Federal Agency for Technical Relief (THW) in disaster relief and infrastructure reconstruction.
Private Sector	The private sector comprises industries, businesses, and all privately owned activities outside direct state control, typically operating for profit.	Private sector actors often own key infrastructure (e.g., transport, telecoms) and can provide critical support in areas such as communication, cybersecurity, and technology. Their involvement in SFA can enhance operational capabilities and resilience of local forces. **Examples:** Microsoft (cybersecurity tools and training for civilian and military organizations).
International Organizations	Organizations established by treaty or other international legal instruments, possessing their own legal personality and often	International organizations can support SFA by strengthening rule of law, security sector governance, and capacity building in host nations. Their missions often

Category	Definition	SFA Connection
	including states and other entities as members (e.g., UN, EU, AU, OSCE, WTO).	complement NATO efforts and provide legitimacy and resources for comprehensive security assistance. **Examples:** EU (EUCAP Sahel missions); African Union (peacekeeping and capacity building in Africa).
Non-governmental Organizations (NGOs)	Private, non-profit organizations independent from government, pursuing activities such as humanitarian aid, poverty alleviation, environmental protection, social services, and community development.	NGOs address humanitarian needs, provide essential services, and support community development, thereby complementing SFA and multi-domain operations (MDO). Their independent operations can fill gaps in governance and public welfare, supporting overall mission success. **Examples:** Médecins Sans Frontières (medical assistance in conflict zones); International Rescue Committee (humanitarian aid and post-conflict recovery).

Chapter 10 — Challenges, Limitations, and Future Directions for SFA in MDO

Maj. Filippo Barone (ITA-A), Author

NATO Security Force Assistance Centre of Excellence (NATO SFA COE), Concept Development & Experimentation Branch, Experimentation Section Chief

10.1 Introduction

This paper has argued that SFA should be recognised as a structural enabler of MDO rather than a supplementary activity, and that this recognition strengthens doctrine, resourcing, and the metrics by which success is measured. The preceding chapters have examined that argument across the operational domains and cross-cutting dimensions that define the contemporary environment. This final chapter does not summarise them. Its purpose is synthesis: to draw together the considerations that recur across domains, to set out plainly the scope of the analysis presented here, and to identify the directions in which SFA is evolving — and should continue to evolve — to meet the demands that MDO places upon it. It is, in this sense, the closing of the circle: the point at which domain-specific findings converge into a single, forward-looking assessment of where the Alliance stands and what can now be done.

The tenor of that assessment is deliberately constructive. The considerations set out below are not failings of the SFA enterprise but the shared agenda of an Alliance in transformation: questions that NATO's commands and its COE network are already engaged in answering.

10.2 Cross-cutting Challenges

Several challenges recur across the domain analyses in this paper. They are not domain-specific difficulties but structural features of SFA in a multi-domain environment, and each is corroborated by sources beyond this study. Taken together, they define the agenda for aligning the SFA enterprise with the ambition of MDO — an agenda common to the Alliance as a whole rather than peculiar to any one nation or institution.

10.2.1 Extending Doctrine Beyond the Land Domain

The most consistent observation across the domain chapters is that dedicated SFA doctrine is most mature in the land domain. Land-based SFA rests on a ratified doctrinal foundation in AJP-3.16; the maritime, air, space, and cyber chapters each noted, in their own terms, that an equivalent body of doctrine for translating MDO requirements into partner force capability development is still taking shape. This is not a peculiarity of NATO's SFA enterprise but a reflection of the broader maturation of the MDO doctrine itself. Independent analysis describes MDO implementation across the Alliance as a work in progress, with common understanding developing at the level of doctrine, processes, and organisation;[397] the Multinational Capability Development Campaign's Multi-Domain Multinational Understanding project reached a similar conclusion, identifying the translation of agreed principles into doctrine, organisation, and training as a priority as early as 2022.[398] The SFA enterprise and the

[397] Calcagno, E. (ed.) (2026). Taking Multi-domain Operations from Theory to Practice. Documenti IAI 26|01. Rome: Istituto Affari Internazionali, February 2026.
[398] Multinational Capability Development Campaign (MCDC) (2022). Multi-Domain Multinational Understanding. November 2022, p. 26. The MMU project, led by the United

operational concept it serves are therefore maturing together, and the most productive course is to develop them in step.

This sequencing has practical implications. While domain-specific SFA doctrine is still developing, advisory work benefits from explicit guidance so that it does not default to the land domain template — emphasising platforms, tactical proficiency, and force generation — in domains where the institutional requirements differ. Recent Alliance-level analysis has set out near- and medium-term priority initiatives for NATO's multi-domain transformation,[399] and the 2025 NATO Multi-Domain Operations Conference in Ankara identified common understanding of MDO across the Alliance as one of three principal priorities, alongside cross-domain command and capability development coordination.[400] The same priorities apply, with equal force, to the SFA enterprise that carries MDO principles to partner nations.

10.2.2 Capability Asymmetry and Co-Development

A second consideration refines the conventional model of SFA as a relationship in which a more capable provider develops the capacity of a less capable partner. In a multi-domain context, advanced capabilities — in space, in cyber, in the integration of unmanned systems — are distributed unevenly not only between NATO and its partners but among

Kingdom and NATO ACT, identified the translation of agreed principles into doctrine, organisation, and training as a priority gap.

[399] Kramer, F. et al. (2024). "NATO Multi-domain Operations: Near- and Medium-Term Priority Initiatives." Atlantic Council Issue Brief, 21 February 2024.

[400] NATO 2025, Allied Command Transformation, "Multi-Domain Operations Conference: Driving Success Across All Domains," 27 May 2025. The Ankara conference identified common understanding of MDO across the Alliance as one of three principal priorities.

Allies themselves. One recent assessment observes that few Allies other than the United States currently possess the full spectrum required to conduct autonomous MDO.[401] Where the providers of SFA are themselves at different stages of multi-domain maturity, the question of what standard partner forces should be assisted toward — and by whom — calls for deliberate coordination.

This asymmetry is best understood, not as a deficiency, but as a condition to be designed around. Germany's defence planning authorities have characterised their own adaptation to a full MDO capability as a marathon requiring a generational timeframe, rather than a sprint;[402] the future of the Alliance is widely understood to depend on precisely this collective adaptation.[403] For SFA, the implication is that partner force development in the newer domains is best framed as co-development along converging paths rather than one-directional transfer — a network of capability development in which Allies and partners advance together. This reframing, from a hierarchy of capability transfer to a network of co-development, is one of the more constructive shifts that this paper identifies.

[401] Calcagno (2026), op. cit. The observation that few Allies other than the United States possess the capabilities to conduct autonomous multi-domain operations is made in the NATO chapter of that study.

[402] Bundeswehr Office for Defence Planning (2024). Multi-Domain Operations for the Bundeswehr: A Short Introduction. March 2024, which characterises German adaptation to a full MDO capability as a "marathon" rather than a "sprint," anticipating a generational timeframe.

[403] Gilli, A. et al. (2025). "NATO, Multi-Domain Operations and the Future of the Atlantic Alliance." Comparative Strategy, 44(1), pp. 73–91.

10.2.3 Governing Commercial Dependencies

The integration of non-military actors, examined in the civil-military chapter and recurring throughout the domain analyses, raises a consideration that SFA doctrine is only beginning to address. In several domains the most consequential capabilities are owned and operated not by states but by commercial entities. The dependence of Ukrainian command and control on a privately owned satellite constellation in 2022 illustrated the strategic significance of this fact. It is not confined to partner nations: NATO itself integrated a commercially developed AI command system — the Maven Smart System NATO — into Allied Command Operations through an exceptionally rapid procurement in 2025.[404] The Alliance, in other words, navigates the same commercial relationships that its SFA programmes help partner nations to manage.

For SFA, this means that capability development is increasingly a trilateral relationship, in which a commercial actor's incentives and policies bear on a partner's operational effectiveness. The synchronisation of military activity with instruments of power that lie outside direct government control is well recognised at the conceptual level;[405] the opportunity now is to translate that recognition into SFA practice. Building a partner force that is resilient in a multi-domain environment increasingly means helping a partner institution to develop the capacity to govern its commercial dependencies — an advisory task of growing importance.

---

[404] Eshel, T. (2025). "NATO AI Modernization: Palantir's Maven Smart System Acquisition." Defence Update, 18 April 2025. The Maven Smart System NATO was integrated into Allied Command Operations at SHAPE through an exceptionally rapid procurement in 2025.

[405] Dailey, A.M. (2023). "NATO Needs a Plan for Military and Nonmilitary Instruments of Power to Work Together." New Atlanticist, Atlantic Council, 2 November 2023.

10.2.4 The Metrics Dilemma

The argument of this paper holds that SFA generates strategic value through institutional resilience, not solely through immediate tactical performance. The domain chapters did not, however, settle how institutional resilience should be measured, and this is the consideration most in need of development. The measures by which SFA is conventionally assessed — personnel trained, equipment delivered, courses completed, exercises conducted — capture activity and output. They do not yet capture whether a partner force can identify threats across domains, decide at the appropriate level and speed, or sustain capability when external support recedes.

Developing measures that complement output with institutional resilience is therefore a priority of real consequence. As long as success is defined mainly by what can be readily counted, advisory effort is naturally drawn toward the tactical; adding an institutional dimension to assessment would help to steer it toward the durable capability that MDO requires. Measures that capture institutional resilience, interoperability maturity, and the capacity for autonomous cross-domain decision-making are thus not a peripheral refinement but a means of aligning the SFA enterprise with its own strategic purpose. Section 10.4.3 sets out four families of indicator through which such measures might be constructed.

10.2.5 The Pace of Technological Change

The cyber and AI chapter observed that the AI-Cyber nexus evolves faster than any doctrinal or planning cycle can readily accommodate, and this extends well beyond the cyber domain. The pace at which unmanned systems, electronic warfare, and AI-enabled decision support are reshaping

the environment means that capabilities which are current at the start of an advisory programme may be superseded before it concludes. Independent analysis cautions, too, that increasingly complex MDO-enabling technologies can render systems impractical to operate or vulnerable to disruption in contested environments.[406]

This temporal feature shapes how SFA is best designed. A programme calibrated to a fixed threat picture transfers a snapshot of capability that begins to depreciate immediately; a programme designed to build adaptive institutions — partner forces able to identify technological change, absorb it, and revise their own doctrine and training in response — transfers something more durable. The distinction maps directly onto this paper's central argument: adaptive institutional capacity, not fixed technical proficiency, is what keeps a partner force relevant as the environment evolves.

10.2.6 The Human and Cultural Dimension

Underlying the preceding considerations is the human dimension, which independent analysis consistently identifies as the most demanding aspect of MDO transformation. Technology can be procured comparatively quickly; the doctrine, training, command culture, and institutional trust required to employ it cohesively will mature over a longer horizon, and some national differences in command culture and military tradition are

[406] Calcagno (2026), op. cit., noting the risk that increasingly complex MDO-enabling technologies "might generate systems that are too impractical to operate or too vulnerable to disruption in contested environments."

expected to endure.[407] What is true for the Alliance's own forces is true also for partner nations whose institutions are still maturing.

This is, in one sense, a demanding conclusion: the most important objectives of SFA in an MDO context are also the slowest to achieve. But it is a clarifying one. It confirms that SFA is fundamentally an institutional enterprise that draws on technology, rather than a technical enterprise that occasionally touches institutions. The human and cultural dimension is not one consideration among several — it is the dimension through which the others are ultimately resolved. Recognising this is the precondition for designing SFA programmes whose ambitions match the timeframes over which institutional change occurs.

10.3 Limitations of This Research

The conclusions of this paper should be read in light of its scope, which is worth stating plainly.

First, the analysis rests on a single principal case study. NMI was selected as an operationally mature mission whose multi-domain context makes abstract doctrinal questions concrete, and the domain chapters drew on evidence beyond it. A single case, however instructive, cannot by itself establish the generalisability of the argument; its conclusions invite testing against other contexts — missions under different political constraints, in different regions, and with partners at different stages of institutional development.

[407] Calcagno (2026), op. cit., observing that some national nuances "will likely endure, due to different national cultures and military traditions," even after a generational adaptation period.

Second, the contributions assembled here reflect the perspectives and analytical depth of distinct institutional authors and are not uniform. Some domains are treated with greater doctrinal specificity than others, partly because the underlying body of doctrine and practice is itself more developed in some domains. This unevenness is, in part, a finding in its own right, mirroring the varying maturity of doctrine across domains.

Third, the cognitive and information dimensions of MDO, while referenced throughout, are not given dedicated treatment in this paper. They cut across every domain and are central to the grey-zone competition that MDO is designed to address adversaries increasingly seek advantage not by defeating forces but by shaping the perceptions, decision-making, and will of institutions and populations. This gap is deliberate rather than overlooked. The NATO SFA COE is addressing it in a dedicated forthcoming study, "SFA Considerations Related to Cognitive Warfare," which will examine how SFA must adapt when the decisive terrain is the human mind — including the STRATCOM perspective through which partner forces communicate, contest hostile narratives, and sustain the trust of their own populations. That study should be read as the natural continuation of the present one, extending the multi-domain argument developed across these chapters into the cognitive dimension. Finally, this paper was written during a period of rapid conceptual and technological change. NATO's MDO concept continues to evolve, partner threat environments are shifting, and the lessons of ongoing conflicts are still being absorbed. The assessments offered here are accordingly a contribution to a developing conversation rather than a settled account of it. These are boundaries of scope, not of confidence in the central argument.

10.4 Future Directions

The considerations identified above are demanding but they are not intractable, and the mechanisms to address them largely already exist. Consistent with this paper's central argument, the directions of effort that follow are organised around the three axes on which the recognition of SFA as a structural enabler of MDO depends: doctrine, resourcing and metrics. They are deliberately cross-cutting rather than domain-specific, since the domain chapters have addressed domain-level requirements in detail. The project-management toolkit presented in Appendix 2 provides practical instruments for operationalising all three.

10.4.1 Doctrine: Developing Multi-Domain SFA through the MDO-enabled Process

The most important instrument for aligning SFA with MDO is one the Alliance already possesses: the Allied Joint Doctrine architecture and the joint, multinational working groups that develop and maintain it. MDO is, by definition, a joint undertaking — the orchestration of effects across services and domains that no single component can deliver alone. It follows that the doctrine governing SFA in a multi-domain context is best developed jointly, through the same interservice and multinational deliberation that produces Allied Joint Doctrine more broadly. Advancing SFA doctrine within the Allied Joint Operations Doctrine (AJOD) framework, rather than in single-service or single-domain isolation, is therefore not merely an administrative preference but a reflection of the nature of MDO itself.

In concrete terms, this means extending the mature foundation of AJP-3.16 across the maritime, air, space, and cyber domains and, above all, capturing

the cross-domain integration that is the essence of MDO. Because AJP-3.16 is part of a coherent joint doctrinal lineage, that extension is best achieved not by drafting separate domain manuals in parallel but by enriching a single joint product — through domain-aware supporting publications developed under the AJP-3.16 lineage and sequenced to mature in step with MDO doctrine rather than after it. It is here that the Centre of Excellence network offers its distinctive contribution: as subject-matter custodians feeding the joint doctrine process, the SFA COE and the domain-specialised Centres — maritime, air, space, cyber, and civil-military — are positioned to bring domain-specific expertise to a common joint table, ensuring that multi-domain SFA doctrine is coherent rather than fragmented. This is the mechanism by which the breadth demonstrated across the preceding chapters becomes a single, integrated doctrinal product.

That the joint approach is sound is increasingly evident in practice. Exercise STEADFAST DUEL 2025 tested the Alliance's collective readiness to integrate effects across domains and commands,[408] demonstrating that multi-domain integration is becoming operational practice and not doctrinal aspiration alone. The lessons drawn from such exercises feed back into the joint doctrine cycle and, through the SFA COE's analysis and lessons-learned pillar, into the way partner forces are advised: sustaining the cycle of learning, changing, and adapting that defines NATO's transformation.

[408] NATO 2025, Allied Command Transformation, "Integration in Motion: NATO's Collective Readiness Tested at STEADFAST DUEL 2025," 4 November.

10.4.2 Resourcing

Resourcing models are most effective when they support institution-building alongside output generation. This means funding sustained advisory engagement as well as discrete training events, supporting long-duration relationships that match the timeframes over which institutional change occurs, and developing a cadre of advisors with the cross-domain expertise that multi-domain SFA requires. It also means accounting explicitly for the commercial dimension: where partner capability depends on private sector providers, advisory effort can extend to building the partner's capacity to govern those dependencies. Resourcing that sustains institutional continuity, and not activity alone, is what converts advisory effort into durable partner capability. In practice this does not require new instruments so much as the deliberate use of existing ones. Multi-year programming under the DCB initiative already permits the funding of sustained engagement rather than discrete events; trust-fund and partner-nation cost-sharing arrangements can underwrite advisory continuity across rotations; and the reach-back and remote advisory arrangements developed by the Centre offer a means of preserving institutional knowledge when deployed presence is reduced. The constraint is less the absence of mechanisms than the tendency to programme against annual activity targets rather than institutional outcomes.

10.4.3 Metrics

Finally, the Alliance can invest in measures of institutional resilience that complement existing output measures. Resilience-oriented indicators would assess a partner force's capacity to identify multi-domain threats, to decide and act at the appropriate level and speed, to protect its own

networks and dependencies, and to sustain and adapt its capability over time. Four families of indicator follow directly from those capacities and are offered here as illustrative rather than prescriptive.

Detection ownership. Rather than counting incidents, assessment can examine whether cross-domain events are first recognised by the partner's own structures or by its advisors — and how that balance shifts over the life of a programme. A partner force that consistently learns of intrusions, interference, or anomalous activity from external mentors has not yet internalised multi-domain awareness, however well equipped it may be.

Decision level and latency. Multi-domain effectiveness depends on decisions being taken at the right level and at acceptable speed. Exercise observation can record the proportion of cross-domain decisions resolved at the level at which doctrine intends them to be resolved, without unnecessary escalation, and the time taken to reach them. Both are observable without additional instrumentation, because exercises already generate the necessary record.

Dependency governance. Where partner capability rests on commercially provided services — satellite communications, network infrastructure, data services — resilience can be assessed through the existence, currency, and rehearsal of contingency arrangements for their degradation or withdrawal, rather than through the presence of the capability alone.

Sustainment and self-revision. The most demanding indicator is also the simplest to state: whether a partner institution can deliver a complete training cycle without external mentoring, and whether it can revise that cycle in response to a changed threat picture. The first tests sustainment;

the second tests adaptation, which is what a rapidly evolving environment ultimately requires.

Indicators of this kind carry familiar risks. They are proxies rather than direct measures, they are more demanding to collect than output counts, and any measure that becomes a target invites optimisation toward the measure itself. These are arguments for developing them carefully and in dialogue with partners, not for continuing to rely on measures that are easy to collect but silent on the question that matters.

A practical first step is to develop and pilot such indicators within an existing, mature mission, refining them through the lessons-learned process before wider adoption. Developing these measures is methodologically demanding, but the effort is worthwhile: what is measured is what is prioritised, and aligning the measurement of SFA with its strategic purpose is among the most consequential refinements recommended by this paper. Appendix 2 offers performance-tracking and assessment templates that can serve as the starting point for such a pilot.

10.5 Conclusion

This paper began with a claim: that SFA is not a supplementary activity adjacent to MDO but a structural enabler of them, and that without resilient and interoperable partner forces, NATO's own multi-domain effectiveness is constrained at its most critical interface — the partner nation. The domain chapters tested that claim against the land, maritime, air, space, and cyber environments and the cross-cutting pressures of climate change and civil-military integration. This final chapter has drawn their findings together.

The conclusion is twofold. The agenda is substantial: SFA doctrine is most developed in the land domain and is still extending across the others; capability is unevenly distributed even among providers; commercial dependencies are only beginning to be governed; success is not yet measured in the terms that matter most; the environment changes faster than doctrine can easily follow; and the institutional change that ultimately determines success is the slowest to achieve. Yet none of these calls for invention from nothing. The direction of effort is clear, and the means largely exist doctrine can extend across domains through the joint working-group process that the COE network already supports; resourcing can sustain institutions as well as outputs; and measurement can be broadened to capture resilience as well as activity. And where this paper stops — at the threshold of the cognitive dimension — the Centre's forthcoming work on SFA and cognitive warfare, encompassing the Strategic Communications dimension of partner-force development, will carry the argument forward into the domain in which future competition may ultimately be decided.

The strategic logic is finally simple. NATO’s ability to conduct MDO does not end at the boundaries of its own forces. It extends to the partners alongside whom the Alliance operates, and it is only as strong as the weakest interface in that network. SFA is the instrument through which that interface is strengthened. Developed jointly across domains and treated as the structural enabler it is — in doctrine, in resourcing, and in the standards by which it is judged — it is an instrument that the Alliance is well placed to wield.

APPENDIX 1 – MDO FORMULA

$$MDO = \left(\sum_{i<j} k_{ij}(X_i \cdot X_j) \right) \times K_{sync}$$

The traditional view that MDO is simply the sum of military domains (land, maritime, air, space, cyber) is misleading. This assumption implies that military effectiveness comes from merely adding capabilities from different domains. However, MDO is fundamentally different from Joint Operations - it is about the orchestration and synchronization of actions across multiple domains and environments to create synergistic effects that exceed the sum of their parts.

To mathematically capture this, we need a formula that:

1. Emphasizes domain integration instead of treating them as isolated contributors.
2. Incorporates synchronization with non-military activities, which is a key differentiator of MDO.
3. Reflects the reality that cross-domain coordination amplifies effectiveness, rather than just summing domain capabilities.

This formula is an illustrative construct rather than an analytical tool. It cannot encompass the complexity of MDO, and the values assigned to capabilities and coefficients in the example that follows are notional. Its purpose is to make explicit, in symbolic form, a proposition that is otherwise easily lost in prose: that multi-domain effectiveness arises from

the interaction between capabilities rather than from their accumulation, and that this structure carries consequences for fragility as well as for advantage.

A note on interpretation: because the formula multiplies pairs of capabilities ($X_i \cdot X_j$), its output is of a different order of magnitude than the naïve sum of individual capabilities. The comparison between the two values that follows should therefore be read as illustrating a difference in structure — interaction versus aggregation — rather than as a literal ratio of magnitudes.

Each component of the formula captures a fundamental aspect of MDO orchestration:

1. $\boldsymbol{X_i, X_j}$ **(Military Domain Capabilities)**
    - These represent the operational capabilities of each domain:
        - Land (L)
        - Maritime (M)
        - Air (A)
        - Space (S)
        - Cyber (C)
    - Instead of summing these domains, we focus on their interactions.

2. k_{ij} **(Domain Interaction Coefficient)**

   - This coefficient (ranging from 0 to 1) represents how strongly two domains are interconnected.
   - If k_{ij}=0, the domains operate independently (like in traditional Joint Operations).
   - If k_{ij}=1, the domains are fully synchronized, achieving maximum cross-domain synergy.
   - Example: A **high** k_{ij} value between Air and Cyber means that air operations depend heavily on cyber warfare for electronic jamming and network targeting.

3. $\sum_{i<j} k_{ij}\ (X_i \cdot X_j)$ **(Multi-Domain Coordination Effect)**

   - Instead of adding domain capabilities, we sum the effects of their interactions.
   - The multiplication $X_i \cdot X_j$ ensures that only strongly integrated domains contribute significantly to MDO effectiveness.
   - If a domain is absent (e.g., Cyber is degraded), its interactions with others also collapse.

4. $i < j$ **(Pairing Condition for Domain Interactions)**

   - Ensures that each pair of domains is considered only once to avoid redundancy.

- Example: Air → Space interaction is counted, but Space → Air is not duplicated.
- A consequence of this structure: any domain pair not explicitly assigned an interaction coefficient is treated as $k_{ij} = 0$ and contributes nothing. This is intentional, not an omission. Under this formula a domain that is present but not integrated with others adds zero to MDO effectiveness — which is precisely the point. Capability that is not integrated is, in multi-domain terms, inert.

5. $\boldsymbol{K_{sync}}$ **(Synchronization Coefficient: 1 to 2)**
   - Represents the level of synchronization between military and non-military activities.
   - $\boldsymbol{K_{sync} = 1}$ → No synchronization (purely military operations).
   - $\boldsymbol{K_{sync} > 1}$→ Military actions are coordinated with Non-Military Instruments of Power amplifying strategic effects.
   - Example: Economic sanctions and cyber warfare synchronized with military strikes can cripple an adversary beyond direct combat effects.

A1.1 Practical Example: NATO Air Campaign in Kosovo (1999)

During Operation Allied Force, NATO launched a 78-day air campaign against Serbian forces to stop ethnic cleansing in Kosovo. This operation serves as a good example of how MDO principles (though not fully conceptualized at the time) were applied in practice.

Applying the MDO Formula

1. **Military Domain Capabilities (X_i, X_j)**
    - Air (X_a): NATO conducted extensive bombing campaigns, targeting military infrastructure.
    - Cyber (X_c): Electronic warfare was used to jam Serbian radars and disrupt command-and-control links. (In 1999 these were predominantly electronic warfare rather than cyber operations in the contemporary sense; the term is used here as a proxy for the modern cyber-electromagnetic domain).
    - Space (X_s): Satellites provided ISR.
    - Land (X_l): Kosovo Liberation Army (KLA) fighters provided intelligence on Serbian troop movements.
    - Maritime (X_m): NATO naval forces in the Adriatic launched cruise missiles and enforced blockades.

Note that although the Maritime domain was active (Xm = 7), its cross-domain interaction coefficients in this campaign were effectively negligible: naval action was conducted largely in parallel rather than in synchronised integration with the other domains. Under the formula, Maritime therefore contributes through its standalone presence but not through cross-domain synergy — which is why it does not appear in the interaction terms below.

2. **Cross-Domain Interactions $\sum_{i<j} k_{ij} \ (X_i \cdot X_j)$:**
    - Air and Cyber (k_{ac}): Electronic-warfare effects disrupted Serbian command and control.
    - Air and Space (k_{as}): Satellite data allowed precision-guided munitions to target Serbian forces.
    - Land and Air (k_{la}): Ground intelligence from KLA fighters improved targeting for NATO bombers.
3. **Synchronization with Non-Military Efforts (K_{sync}):**
    - Diplomacy: UN and NATO worked in parallel to negotiate Serbian withdrawal.
    - Economic: Trade sanctions weakened Serbia's war economy.

- Media & Information: Western media framed the intervention as a humanitarian necessity, influencing public and diplomatic support.

Serbia's withdrawal from Kosovo was achieved without the deployment of ground forces, in a campaign that combined military action with sustained diplomatic and economic pressure. Historians continue to debate the relative weight of these factors; the campaign is used here not to settle that question, but because it offers a well-documented case in which effects across several domains were pursued alongside non-military instruments.

A1.2 Mathematical Representation

Given the domain capabilities:

$X_a = 12;\ X_c = 3;\ X_s = 6;\ X_l = 5;\ X_m = 7$

And the interaction coefficients:

$\boldsymbol{k_{ac}} = 0.8$; $\boldsymbol{k_{as}} = 0.9$; $\boldsymbol{k_{la}} = 0.7$

With a synchronization coefficient of $\boldsymbol{K_{sync}} = 1{,}5$ (due to strong diplomatic and economic pressure), the **MDO value** is calculated as:

$$MDO = [0.8(12 \times 3) + 0.9(12 \times 6) + 0.7(5 \times 12)] \times 1.5$$

$$MDO = (28.8 + 64.8 + 42) \times 1.5$$

$$MDO = 203.4$$

This high value illustrates how cross-domain synergy and synchronisation with non-military activities can be represented as amplifying the overall effect of a campaign. The coefficients used here are assigned retrospectively for illustrative purposes and are not derived from campaign

data: the formula therefore represents the structure of the relationship rather than measuring it, and the value obtained should not be read as an explanation of the campaign's outcome.

For comparison, if MDO were treated as the simple sum of the domains, the result would be:

$$MDO = 12 + 3 + 6 + 5 + 7 = 33$$

As noted above, these two values are not directly comparable: the first is built from products of capabilities, the second from their sum, so they belong to different orders of magnitude. The contrast is presented to illustrate the difference between an interaction-based and an aggregation-based conception of multi-domain effectiveness, not to quantify the advantage of one over the other.

A1.3 The Fragility of Multi-Domain Integration: A Degradation Scenario

The same formula that explains MDO's amplifying power also explains its fragility. Because effectiveness is generated through interactions rather than standalone contributions, degrading a single domain does not subtract that domain's nominal value — it removes every interaction that depended on it.

Consider what happens to the Kosovo result if the Cyber/EW domain is denied. The Air–Cyber interaction term (28.8) collapses entirely, leaving:

$$MDO = [(0.9 \cdot 12 \cdot 6) + (0.7 \cdot 5 \cdot 12)] \times 1.5$$
$$= (64.8 + 42) \times 1.5 = \mathbf{160.2}$$

The loss is **43.2** — yet the standalone value assigned to Cyber was only 3. Degrading a single domain therefore produced a loss roughly fourteen times greater than that domain's nominal contribution, because the value destroyed lay not in the domain itself but in the interactions it enabled.

The effect is even more pronounced for a highly connected domain. In this example, every interaction term passes through the Air domain, which functions as the integrating hub. If Air is denied, all three interaction terms collapse and the result falls to **zero**, regardless of how capable the other four domains remain individually. This is the mathematical expression of a central operational reality: adversaries do not need to defeat a multi-domain force across every domain. They need only to degrade the domains through which integration flows. It also explains why the enabling domains — space, cyber, and the command-and-control links that bind the others together — are the priority targets in contemporary conflict, and why SFA that builds resilience in precisely these connective domains is disproportionately valuable.

APPENDIX 2 - PROJECT MANAGEMENT FOR SFA DELIVERY IN MDO

Maj. Biagio Ferrante (ITA-A), Author

NATO Security Force Assistance Centre of Excellence (SFA COE),

Financial Controller

A2.1 Introduction and Rationale

The strategic case for treating SFA as a structural enabler of MDO is made in the body of this paper. This appendix addresses a complementary and deliberately practical question: how SFA activities can be managed — planned, governed, executed, and measured — in environments defined by multiple domains, multiple stakeholders, and finite resources. Its answer draws on the discipline of project management, whose established methodologies — ISO 21502, PRINCE2, the PMBOK® Guide, PM², Scrum, and Six Sigma — offer structured approaches to precisely the challenges that recur throughout this study: coordination across organisational boundaries, governance and accountability, risk management, and the measurement of progress.

The need is a direct consequence of the operational picture described by the preceding chapters describe. MDO implementation requires the interoperability of multiple systems, forces, and technologies, aligned with strategic purposes; and SFA adds a further layer of complexity, because civilian and military actors alike become part of the decision process.[409]

[409] Sleevi, N.F., & Byrd, J.A. (2022). "Security Force Assistance: Enabling Foreign Security Forces Integration into Multi-Domain Operations." SFA Quarterly, 24th ed., September 2022.

SFA initiatives are multi-theatre and multi-stakeholder by nature, requiring careful coordination among governments, IOs, NGOs, and the host nation. Project management methodologies offer a common language and a shared toolset — Work Breakdown Structures, Key Performance Indicators, risk registers, responsibility matrices — through which these diverse actors can pursue a common goal with transparency and accountability.

This appendix is conceived as a companion to Chapter 10. Where that chapter identifies doctrine, resourcing, and metrics as the axes along which SFA must evolve to serve a multi-domain Alliance, the pages that follow supply practical instruments for operationalising those directions. The material is equally relevant to the NMI case examined in Chapter 3 — from which the case study below is drawn — and to the civil-military coordination challenges analysed in Chapter 9.

A2.2 Scope and Methodology

The analysis rests on a comparative method that identifies conceptual and structural correspondences between NATO operational planning doctrine — principally AJP-5 and the Comprehensive Operations Planning Directive (COPD) — and internationally recognised project management standards.[410] The comparison is not intended to equate military and civilian systems, but to examine systematically how analogous structures, processes, and decision-making mechanisms operate across different institutional contexts, and to identify tools — stakeholder maps, Key

[410] George, A.L., & Bennett, A. (2005). Case Studies and Theory Development in the Social Sciences. Cambridge, MA: MIT Press.

Performance Indicators, Work Breakdown Structures, risk registers — that can be transferred between them.

ISO 21502:2020 is adopted as the primary reference framework. The choice reflects the standard's deliberate generality: it is "applicable to any organization … irrespective of complexity, size or duration,"[411] which provides the rationale for employing civilian project management frameworks as an analytical lens for military operations. The practical output of the approach is a set of field-adaptable templates — stakeholder analyses, risk management plans, project charters, and performance-tracking tools — designed to be interoperable with military planning processes and consistent with the Alliance's enduring commitment, reaffirmed at the Warsaw Summit, to enhancing partner support through DCB.[412]

A2.3 Project Management Methodologies: Overview and Military Relevance

Six methodologies have been selected for their relevance, adaptability, and complementarity with military planning and execution models. They are treated not as rigid or standalone frameworks but as reference models whose principles, governance mechanisms, and tools can be selectively adapted to mission requirements, operational tempo, and stakeholder configuration.

[411] International Organization for Standardization, ISO 21502:2020 — Guidance on Project Management, https://www.iso.org/standard/74947.html.

[412] NATO 2016, Warsaw Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2016.

ISO 21502:2020 provides a global standard for project governance and delivery, focusing on alignment with organisational strategy, roles, and accountability; this is particularly valuable for defence cooperation frameworks, host-nation engagement, and institutional reform programmes. PRINCE2 offers a structured, process-oriented framework whose modular and hierarchical logic mirrors military command structures, making it well suited to phased operations with strict reporting requirements. The PMBOK® Guide, published by the Project Management Institute, emphasises standardisation through process groups and knowledge areas that align with NATO's operational design and planning doctrine, especially in multinational and interagency environments.[413] PM², developed by the European Commission, combines predictive and agile elements with a strong focus on stakeholder engagement and layered governance and is well aligned with CIMIC settings where coordination with civilian actors and public administrations is fundamental. Scrum is a lightweight, iterative framework suited to rapidly evolving environments such as cyber defence activities and technology-driven experimentation. Six Sigma, built on the DMAIC cycle (Define, Measure, Analyse, Improve, Control), lends its analytical rigour to logistics, procurement, and sustainment functions.

The following table summarises the principal areas of alignment across these methodologies.

[413] Project Management Institute (2021). The Standard for Project Management and A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 7th edition.

Area	Involved methodologies	Comment
Business justification	PRINCE2, PM², PMBOK, ISO 21502	Continuous value and purpose alignment.
Phased management	PRINCE2, PM², ISO 21502, PMBOK	Projects structured and executed in controlled stages.
Defined roles and responsibilities	PRINCE2, PM², PMBOK, ISO 21502	Clear team structures and accountability.
Tailoring to context	PRINCE2, PM², PMBOK, ISO 21502	Adaptation to the organisation, team, and environment.
Focus on deliverables	PRINCE2, PM², ISO 21502	Emphasis on tangible outputs that meet specifications.
Stakeholder engagement	PMBOK, PM², ISO 21502, PRINCE2	Prioritising stakeholder needs, expectations, and communications.
Value and benefit focus	PMBOK, PRINCE2, ISO 21502, Six Sigma	Projects must deliver measurable value or improvement.
Quality and process control	PMBOK, Six Sigma, ISO 21502	Structured tools and metrics for monitoring and control.
Iterative learning and adaptation	Scrum, PMBOK, ISO 21502	Agile responsiveness to change and complexity.

A2.4 Convergences between NATO Doctrine and Project Management

NATO military doctrine and formal project management share several foundational principles, creating a natural synergy between military planning and structured project methodologies. Both define clear objectives and scope: AJP-01 provides the fundamental principles by which Allied forces guide their actions in support of objectives, and project management likewise defines purpose, scope, and deliverables at the outset. Both clarify roles and responsibilities: the military principle of unity of command is mirrored in the governance structures and accountability chains of PRINCE2 and PMBOK. Both prioritise structured risk management — NATO's alignment with ISO 31000 for risk frameworks parallels the risk registers and mitigation planning at the core of project methodologies.[414] Both institutionalise learning: NATO's Lessons Learned Process is built on the same continuous feedback and corrective action embedded in project retrospectives. The military concept of Mission Command — empowering subordinate leaders to act within the commander's intent — is echoed in agile methods such as Scrum, which combine decentralised decision-making with structured oversight. And both standardise processes for coherence and interoperability: NATO's STANAGs perform the same function for the Alliance that ISO 21502 and the PMBOK® Guide perform for the project management profession.

This convergence demonstrates that project management is not merely administrative but deeply aligned with military doctrine. Defence planners

[414] International Organization for Standardization, ISO 31000:2018 — Risk Management: Guidelines

can leverage the overlap explicitly, integrating project management structures into NATO and national planning cycles — AJP-5, the COPD, and Annex W — to strengthen complexity management in MDO.

A2.5 Project Management in the MDO Context

Integrating project management into MDO environments is a conceptual evolution rather than a procedural adaptation. Three dimensions matter most. First, alignment: every initiative must contribute directly to operational and strategic effects across domains, which means that project charters and SMART objectives must be calibrated to systemic, cross-domain effects rather than isolated outputs — a cyber defence training initiative, for example, should be scoped for its contribution to space and information resilience, not merely its immediate deliverable. Second, synchronisation: time-phased implementation plans, Work Breakdown Structures with explicit interdependencies, and milestone-based reviews allow the delivery of a capability to be synchronised with enabling actions in adjacent domains, while RACI matrices and dependency maps assign responsibilities across domain-specific stakeholders. Third, decentralised execution: the MDO environment is too complex for centralised control alone, and project governance must therefore embody Mission Command — defining intent, autonomy boundaries, risk thresholds, and escalation protocols so that local implementers can adjust rapidly without compromising coherence.

A2.6 Doctrinal and legal anchoring

Project management in military environments must be rooted in doctrinal legitimacy and legal robustness. Doctrinally, project-based activities are embedded within the framework provided by AJP-01, the operational and campaign-level planning of AJP-3 and AJP-5, the COPD, and — for CIMIC and SFA delivery mechanisms — Annex W of NATO operation plans. ISO 21502 complements this architecture by defining roles such as project sponsor, project board, and project manager, clarifying decision-making responsibilities and accountability chains that are particularly valuable where projects are subject to multinational oversight and host-nation legal scrutiny.

In deployed operations, legal considerations weigh heavily. Host-nation law must be respected with regard to public procurement and acquisition regulations, often shaped by national sovereignty or Status of Forces Agreements: labour and employment law when contracting local services; environmental regulations in infrastructure and engineering projects; and anti-corruption and financial compliance, especially where funds are disbursed under cooperative security programmes. Military project managers must therefore coordinate with legal advisors and procurement officers from the earliest stages of project design, and project documentation must consistently reference NATO Financial Regulations, Financial Administrative Procedures, and the host nation's acquisition framework. The combined use of doctrinal structures and internationally accepted standards enables mission effectiveness, transparency, auditability, and legal integrity: critical features for operational legitimacy and long-term strategic partnership.

A2.7 The Project lifecycle in Military Operations

Initiation. Projects in SFA and CIMIC settings emerge from operational needs and are designed to support the force's objectives while fostering resilience within the host nation. Feasibility is assessed against SMART criteria — with attention to collateral effects, local sustainment capacity, and non-dependency on military forces — and stakeholder mapping anticipates political, legal, and cultural sensitivities. Authorisation is formalised through a Project Initiating Document (PID) integrating host-nation consent, command endorsement, and resource commitments.

Planning. The project concept is converted into a structured roadmap using Work Breakdown Structures for the decomposition and delegation of deliverables, Gantt charts aligned with operational phases, a risk matrix identifying potential disruptions — budget shortfalls, scope changes, host-nation political instability — and a communication plan tailored to audience sensitivity and operational security.

Execution and monitoring. Roles and responsibilities are structured through RACI matrices, promoting accountability in joint and interagency environments; progress is monitored through KPIs covering schedule adherence, quality benchmarks, budget performance, and responsiveness to host-nation feedback.

A recurring challenge in this phase deserves particular attention: the impact of personnel turnover on project continuity. Rotational deployments, standard practice in advisory missions, often result in the fragmentation or loss of critical information about project progress, stakeholders, and objectives — a problem exacerbated where projects are managed through ad hoc, non-standardised tools, since successive rotations may employ

divergent approaches. The adoption of standardised methodologies and structured artefacts (PID, RACI matrix, risk register, Gantt charts) ensures consistency of documentation, enhances knowledge transfer, and accelerates the onboarding of incoming personnel. Reach-back arrangements such as Remote SFA further support continuity by preserving institutional knowledge and providing ongoing advisory support beyond the limits of individual rotations.[415]

Control and adaptation. Regular status reviews assess deviations and authorise course corrections; changes to scope, resources, or timelines require documented justification; audits track delivery against KPIs and contractual compliance; and lessons learned are systematically captured and fed into NATO's lessons-learned architecture and institutional memory.

Closure. The closure phase ensures continuity and institutionalisation within the host nation: formal handover to local authorities — critical for ownership, sustainability, and exit strategy — final documentation and financial closeout, and post-project evaluation whose findings feed strategic planning and doctrinal refinement.

Across this lifecycle, the principle of continued business justification — central to PRINCE2, PM², and ISO 21502 — finds its military counterpart in Military Cost-Benefit Analysis, which assesses whether the expected operational, strategic, and political benefits of an action justify the resources, time, and risk allocated, incorporating intangible factors such as

[415] NATO 20204, Security Force Assistance Centre of Excellence. Remote SFA: Reach-Back Capabilities Analysis Report.

host-nation legitimacy and population support.[416] Embedding this shared value logic in project documentation — the PID, monitoring and evaluation plans, and cost-benefit records — allows military and civilian stakeholders to converge on a common, defensible rationale, particularly valuable in politically or fiscally constrained contexts.

A2.8 Governance, Integrity and Risk

Project approval and authorisation in military contexts is a decision process, not a formality. The approval path typically proceeds through successive levels of scrutiny — tactical (the CIMIC or SFA branch), operational (J5 or J9 functional authorities), and strategic or political authorisation by higher headquarters — with each level evaluating feasibility, alignment with planning priorities, resource availability, and risk exposure.[417] Early and continuous involvement of the host nation is critical: projects affecting civil infrastructure, essential services, or governance must be coordinated with local authorities to ensure legitimacy, prevent duplication, and reinforce ownership.[418]

Integration with host-nation structures and civil agencies begins at initiation, where stakeholder mapping and needs assessments are coordinated with ministries, local authorities, and civil society, and efforts are aligned with national development plans to avoid parallel systems that would undermine institutional legitimacy. NATO's approach to civil-

[416] Melese, F., Richter, A., & Solomon, B. (eds.) (2015). Military Cost-Benefit Analysis: Theory and Practice. London: Routledge.
[417] Joint Center for International Security Force Assistance (JCISFA) (2016). SFA Planner's Guide.
[418] NATO Allied Command Operations, ACO Manual 86-1-1: CIMIC Tactics, Techniques and Procedures.

military interaction stresses a synchronised engagement framework: regular liaison, shared information environments, joint assessment mechanisms, and collaborative project boards.[419] Project managers must be prepared to adapt formats, timelines, and reporting procedures to the host environment's political, administrative, and cultural realities while maintaining accountability and mission standards.

Within this governance architecture, procurement deserves specific attention, because in fragile and post-conflict environments it is a strategic enabler that directly affects mission credibility, partner trust, and institutional sustainability. NATO's BIP provides the doctrinal and practical framework for mitigating corruption risk in defence and security procurement, emphasising institutional resilience, transparent acquisition practices, and national capability to manage defence resources accountably.[420] In project terms, integrity is embedded through concrete instruments: corruption-risk clauses in the PID and the risk matrix, transparency benchmarks, competitive bidding, third-party verification, and defined roles for independent monitoring. A dual-track approach — strengthening procurement legislation and oversight on one side, mentoring supported institutions in transparent acquisition practice on the other — treats integrity-building as a continuous process rather than a one-time intervention, consistent with the Centre's own work on the rule of law and good governance.[421] Anti-corruption, in this framing, is not a

[419] Civil-Military Cooperation Centre of Excellence (2024). CIMIC Handbook.
[420] NATO 2021, NATO Building Integrity Policy
[421] NATO 2021, Security Force Assistance Centre of Excellence. Promoting the Rule of Law and Good Governance: SFA Implications in International Initiatives.

secondary concern but a core component of resilience and operational success.

A2.9 Bridging AJP-5 Planning and Project Management

AJP-5 and the COPD articulate operational-level planning through seven phases: initiation, mission analysis, course of action (COA) development, COA analysis, COA validation and comparison, the commander's COA decision, and plan development. These phases have recognisable counterparts in project management. Initiation aligns with PM²'s Initiating phase and PRINCE2's Starting Up a Project; mission analysis corresponds to early planning, where scope, risks, and stakeholder needs are identified; COA development parallels the exploration of delivery options and resourcing models; COA analysis and validation echo structured evaluation stages such as risk assessment and performance simulation; the commander's decision mirrors governance checkpoints such as PRINCE2's Directing a Project or PM²'s steering-committee decisions; and plan development leads to formal planning documents — the OPLAN and its annexes — analogous to integrated project plans. The purpose of the mapping is not to enforce a rigid equivalence but to identify shared principles and transferable tools that facilitate coordination between military planners and civilian institutions operating under project management norms.

Within the planning process itself, the SFA subject-matter expert embedded in the Joint Operations Planning Group applies techniques — capability assessment, factor analysis, centre-of-gravity analysis, and institutional diagnostics using the DOTMLPFI framework — that strongly

resemble project scoping, stakeholder analysis, and gap identification in modern project management.[422] Synchronisation with the OPLAN is achieved principally through Annex W, the designated annex for CIMIC and, increasingly, SFA-related functions: it defines the structure, tasks, timelines, coordination mechanisms, and resource needs of enabling activities, giving them visibility and legitimacy within the joint planning process and across rotations. Standard operating procedures derived from the OPLAN then translate strategic intent into actionable steps — flexible enough to accommodate host-nation capacity and cultural context, while remaining anchored in NATO planning logic. Well-managed projects, when they are synchronised with the battle rhythm and operational phasing in this way, also generate economy of force: by enabling host nation actors to assume critical functions, they free coalition resources for higher-priority tasks.

A2.10 Case Study: NMI support to the Iraqi Military Medical School

The following case illustrates the application of these principles within the mission examined in Chapter 3. In October 2024, NMI delivered medical training equipment to the Iraqi Military Medical School (IMMS) as part of a broader effort to build sustainable military medical capability under NATO's Defence Capacity Building framework.[423] The project fell within the Joint Action Plan between the Iraqi Ministry of Defence, the Ministry

[422] NATO 2023, Security Force Assistance Centre of Excellence. SFA for Planners.
[423] NATO 2024, Mission Iraq. "NMI Provides Iraqi Military Medical School with Training Equipment,"

of Interior, and NMI, contributing to the Long-Term Objective dedicated to the enhancement of branch and service schools — under which curricula are reviewed and training capabilities developed to deliver standardised, NATO-aligned PME.[424] The analysis below assesses the project against ISO 21502, while noting that other methodologies could be adapted to the same context.[425]

Initiation. The project objective was to enhance the educational and operational capability of the IMMS through the delivery of NATO-standard medical training equipment and associated curriculum development, with a specific focus on Tactical Combat Casualty Care (TCCC). The justification rested on strengthening Iraqi defence institutions, increasing interoperability with NATO medical doctrine, and enabling a sustainable, self-owned training capacity within the Iraqi Armed Forces.[426] Stakeholders were identified and engaged from the outset, as summarised below.

Stakeholder	**Role / interest**
NATO Mission Iraq (NMI)	Project owner and strategic coordinator; doctrinal guidance, planning, and oversight.
NMI Defence Capacity-Building Office	Long-term planning and engagement with Iraqi institutions; sustainability and policy alignment.
NMI Medical Advisor (Training Development Division)	Subject-matter expert ensuring doctrinal alignment with NATO TCCC standards.

[424] NATO, Defence and Related Security Capacity Building (DCB) Initiative
[425] NATO Mission Iraq, Overview
[426] International Organization for Standardization, ISO 21502:2020, op. cit.

Implementing partner (NGO)	Procurement and logistical delivery of medical equipment in compliance with NATO requirements and Iraqi regulations.
Iraqi Military Medical School (IMMS)	End user and national beneficiary; training implementation and capability retention.
Iraqi Ministry of Defence / Government Contracts Department	Institutional authority for compliance, approval, and alignment with national procedures.
Mobile Advisory Training Team (NMI)	Delivery of the Train-the-Trainer course to build self-sustaining instructional capability.

Procurement as a project enabler. Procurement proved to be the critical-path activity. Procurement of medical and military-related equipment in Iraq is governed by layered national regulations — customs clearance, import licensing, and technical approvals overseen by the General Government Contracts Department — with heightened sensitivity toward foreign-sourced medical equipment and a real risk of delay or rejection if stakeholders are not engaged early. The mission addressed these constraints by working through an implementing partner with prior operational experience in Iraq, which vetted suppliers holding licences recognised by Iraqi health authorities, coordinated with customs and regulatory bodies, and ensured that all items met both NATO training specifications and IMMS curricular needs. Managed in this way, procurement was not a logistical afterthought but the enabler on which curriculum development, Train-the-Trainer delivery, and long-term local ownership all depended.

Planning through closure. The work breakdown comprised needs assessment and stakeholder coordination; procurement planning and

contracting; logistics and delivery; the handover ceremony; design and delivery of the TCCC Train-the-Trainer course; monitoring of training outcomes and equipment utility; and planning for a second delivery phase. The first equipment shipment was delivered on 14 October 2024, followed immediately by the Train-the-Trainer course (15–30 October 2024) led by a Mobile Advisory Training Team, with Iraqi instructors demonstrating CPR training tools supported by mobile feedback applications. Monitoring combined qualitative indicators — the effective use of equipment in medical simulation and the alignment of the curriculum with NATO standards — with quantitative ones, principally the number of Iraqi instructors trained and the scalability of course delivery across the Iraqi Armed Forces. Phase-one closure included assessment of training outcomes, documentation of lessons learned, and preparation of the follow-on delivery, with sustainability anchored in the Train-the-Trainer model, the integration of digital feedback tools, and continued mentoring by NMI advisors.

Read against ISO 21502, the project displays the standard's essential features: alignment with strategic goals (NATO capacity building and interoperability with the Iraqi Ministry of Defence); structured stakeholder engagement across NATO, Iraqi, and implementing-partner actors; a clear phased lifecycle from needs assessment to follow-up; governance and accountability retained by the mission with execution delegated and host-nation validation preserved; and an explicit sustainability and transition strategy. It therefore offers a concrete demonstration of how structured project management, applied within an SFA mission, converts assistance into durable, locally owned capability.

A2.11 Methodologies at a Glance

The table below condenses the six reference methodologies, their core principles, and their most natural military applications.

Methodology	Core principles	Indicative military application
PRINCE2	Continued business justification; learn from experience; defined roles; manage by stages and by exception; focus on products; tailoring.	Phased SFA operations, force development, modular capability delivery.
PMBOK® Guide (7th ed.)	Stewardship; collaborative teams; stakeholder engagement; value focus; systems thinking; leadership; tailoring; quality; complexity; risk; adaptability; change enablement.	Joint interagency operations; coordination with host-nation ministries.
ISO 21502:2020	Leadership and accountability; stakeholder engagement; strategic alignment; lifecycle management; benefits orientation; governance and transparency; tailoring.	Structured capability development; strategic defence reform; institutional capacity building.
PM²	Business justification; defined roles; manage by phases and by exception; focus on deliverables; tailoring; stakeholder communication.	Interagency missions; civil-military capacity initiatives; post-conflict stabilisation.
Scrum	Transparency, inspection, adaptation; commitment, courage, focus, openness, respect.	Advisory teams in rapidly evolving settings; cyber defence activities; rapid concept development and experimentation.
Six Sigma	Customer focus; data-driven decisions; process improvement and variation reduction; DMAIC cycle.	Operational sustainment; logistics process optimisation; base support improvement.

Templates derived from these methodologies — project initiating documents, stakeholder maps and communication plans, Gantt and Work

Breakdown Structures, SMART-objective checklists, RACI matrices, and risk registers — are maintained by the NATO SFA Centre of Excellence for field adaptation. Used alongside the doctrinal anchors described above, they give practitioners a ready-made bridge between the strategic directions set out in Chapter 10 and the daily management of SFA delivery in a multi-domain environment.

References

- Abels, J. and Bieling, H.-J. (2023) ‘Infrastructures of globalisation: shifts in global order and Europe’s strategic choices’, Competition & Change, 27(3–4), pp. 516–533.

- Atlantic Council (2024) NATO Multi-domain Operations: Near- and Medium-Term Priority Initiatives. Washington, DC: Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-multidomain-operations/

- BBC News (2007) China confirms satellite downed. Available at: http://news.bbc.co.uk/2/hi/asia-pacific/6289519.stm

- Bojor, L. et al. (2024) ‘Emerging Technologies in Conflict: The Impact of Starlink in the Russia–Ukraine War’, Revista Academiei Forţelor Terestre, 29(2), pp. 185–194. Available at: https://doi.org/10.2478/raft-2024-0020

- Cannon, S. (2023) The Alliance’s Transition to Multi-Domain Operations: An AIRCOM Perspective. Ramstein: NATO Allied Air Command.

- Centre for Strategic and International Studies (CSIS) (2025) Space Threat Assessment 2025. Washington, DC: Centre for Strategic and International Studies.

- CIMIC Centre of Excellence (2025) Civil-Military Cooperation Publications. Available at: https://www.cimic-coe.org/

- CNA Military Advisory Board, National Security and the Accelerating Risks of Climate Change, 2014, Available at: https://www.cna.org/reports/2014/MAB_5-8-14.pdf

- Council of the European Union (2008) Operation Atalanta (EUNAVFOR Somalia). Brussels: Council of the European Union.

- Council of the European Union (2021) Coordinated Maritime Presences in the Gulf of Guinea, Council Decision (CFSP) 2021/103. Brussels: Council of the European Union.

- Council of the European Union (2023) European Peace Facility: Assistance Measure in Support of Military Actors and Navies of Gulf of Guinea Coastal States. Brussels: Council of the European Union.

- Council of the European Union (2024) EUNAVFOR Aspides, Council Decision (CFSP) 2024/583. Brussels: Council of the European Union.

- DCAF, 2022, DCAF – Geneva Centre for Security Sector Governance (2022). "Security Sector Reform: Applying the Principles of Good Governance to the Security Sector." SSR Backgrounder Series, DCAF, Geneva.

- Deloitte (2025) Global Cyberthreat Intelligence. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-annual-cyber-threat-trends-report-2025.pdf

- European Commission (2023) EU Civilian and Military Missions and Operations. Available at: https://commission.europa.eu/strategy-and-policy/eu-civilian-and-military-missions-and-operations_en

- European Commission (2025) Cyber Resilience Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

- European Commission (2025) European Defence Fund: Over €1 Billion to Drive Next-Generation Defence Technologies and Innovation. Available at: https://defence-industry-

space.ec.europa.eu/european-defence-fund-over-eu1-billion-drive-next-generation-defence-technologies-and-innovation-2025-01-30_en

- European Council (2022) EU Support to Ukraine: Military Assistance and Training Missions. Available at: https://www.consilium.europa.eu/en/policies/eu-support-ukraine/

- European Defence Agency (2025) Trustworthiness for AI in Defence. Brussels: European Defence Agency. Available at: https://eda.europa.eu/docs/default-source/brochures/taid-white-paper-final-09052025.pdf

- European Parliament (2023) EU Space Strategy for Security and Defence. Available at: https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en

- European Parliament (2024) AIDA – Special Committee on Artificial Intelligence in a Digital Age. Available at: https://multimedia.europarl.europa.eu/en/topic/aida-special-committee-on-artificial-intelligence-in-digital-age_16506

- European Parliament (2025) Defence and Artificial Intelligence. Brussels: European Parliamentary Research Service. Available at:

https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf

- European Union (2025) Artificial Intelligence Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

- European Union Agency for the Space Programme (EUSPA) (2023) GNSS Vulnerabilities Report. Prague: European Union Agency for the Space Programme.

- French Ministry for the Armed Forces (2020) France Launches its Space Command. Paris: Ministry for the Armed Forces. Available at: https://www.defense.gouv.fr/actualites/il-y-cinq-ans-france-lancait-son-commandement-lespace

- French Ministry for the Armed Forces (2024) Commandement de l'Espace: les enjeux de la sécurité spatiale. Paris: Ministry for the Armed Forces. Available at: https://www.defense.gouv.fr/actualites/commandement-lespace-enjeux-securite-spatiale

- Genesys Defense and Technologies. The Evolution of Intelligence Sharing among Military Alliances. Available at: https://genesysdefense.com/intl/the-evolution-of-intelligence-sharing-among-military-alliances

- Godzimirski, J., Bârgăoanu, A. and Ceuca, R. (2024) FLANKS 2 – Addressing the Challenge of Russian Hybrid Warfare the NATO Way: The Case of Norway and Romania. Available at: https://newstrategycenter.ro/wp-content/uploads/2024/10/FLANKS-2-working-paper-2.pdf

- Hajjar, R. (2014) 'What lessons did we learn (or re-learn) about military advising after 9/11?', Military Review.

- Harris, K. (2023) Fact Sheet: Strengthening U.S. International Space Partnerships. Washington, DC: The American Presidency Project. Available at: https://www.presidency.ucsb.edu/documents/fact-sheet-strengthening-us-international-space-partnerships

- Hooker, R. and Collins, J. (2015) Lessons Encountered: Learning from the Long War. Washington, DC: National Defense University Press.

- Hybrid CoE. About Us. Available at: https://www.hybridcoe.fi/about-us/

- Institut Français des Relations Internationales (IFRI) (2025) Tourret, Design, Destroy, Dominate: The Mass Drone Warfare as

a Potential Military Revolution. Available at: https://www.ifri.org/en/papers/design-destroy-dominate-mass-drone-warfare-potential-military-revolution

- International Monetary Fund (IMF) (2024) Container Shipping Disruptions and the Red Sea Crisis. Available at: https://www.imf.org/en/blogs/articles/2024/03/07/red-sea-attacks-disrupt-global-trade

- Jackson P. 2018 Paul Jackson (2018). "Introduction: Second-Generation Security Sector Reform." Journal of Intervention and Statebuilding, Vol. 12, No. 1, pp. 1–10.

- Janes (2025) Ukraine to Receive Starlink Services Under US Deal. London: Janes. Available at: https://www.janes.com/osint-insights/defence-news/air/ukraine-to-receive-starlink-services-under-us-deal

- Joint Air Power Competence Centre (JAPCC) (2023) The Space Domain: A Global Vision. Kalkar: NATO JAPCC. Available at: https://www.japcc.org/articles/space-domain-a-global-vision/

- Joint Air Power Competence Centre (JAPCC) (2024) Collective Defence in the Space Domain. Kalkar: NATO JAPCC. Available at: https://www.japcc.org/articles/collective-defence-in-the-space-domain/

- Knox, M. and Murray, W. (2001) The Dynamics of Military Revolution, 1300–2050. Cambridge: Cambridge University Press.

- Lenoir, D.A. (2023) '571 MSAS Air Advisors: Tactical Actors on a Strategic Level', SFA Quarterly, 26th Edition. Available at: https://www.nsfacoe.org/wp-content/uploads/2023/03/SFA-Quarterly-Newsletter-26th-Edition-March-23-Minimum-Resolution-1.pdf

- Leonardo (2024) Multi-domain Technologies to Address Future Operational Scenarios. Rome: Leonardo.

- Lopez, C.T. (2021) DOD, Navy Confront Climate Change Challenges in Southern Virginia. Washington, DC: U.S. Department of Defense.

- Matisek, J., Messenger, A. and Belohlavek, C. (2025) No More Train and Pray: The Consequences of Cutting the Army's Security Force Assistance Capability. West Point, NY: Modern War Institute. Available at: https://mwi.westpoint.edu/no-more-train-and-pray-the-consequences-of-cutting-the-armys-security-force-assistance-capability/

- Matisek & Reno, 2019, Jahara Matisek & William Reno (2019). "Getting American Security Force Assistance Right: Political Context Matters." Joint Force Quarterly, No. 92, pp. 65–73

- MISP (n.d.) MISP Open Source. Threat Intelligence Platform & Open Standards for Threat Information Sharing. Available at: https://www.misp-project.org/

- NASA (2020) The Causes of Climate Change. Washington, DC: National Aeronautics and Space Administration. Available at: https://climate.nasa.gov/causes/

- NATO (2011) Alliance Maritime Strategy. Brussels: North Atlantic Treaty Organization.

- NATO (2019) NATO's Overarching Space Policy. Brussels: North Atlantic Treaty Organization. Available at: https://www.nato.int/cps/en/natohq/topics_175419.htm

- NATO (2021) Brussels Summit Communiqué. Brussels: North Atlantic Treaty Organization. Available at: https://www.nato.int/cps/en/natohq/news_185000.htm

- NATO (2021) NATO Climate Change and Security Action Plan. Brussels: North Atlantic Treaty Organization.

- NATO (2022) Allied Joint Publication (AJP)-01: Allied Joint Doctrine. Brussels: North Atlantic Treaty Organization.

- NATO (2022) Allied Joint Publication (AJP)-3.2: Allied Joint Doctrine for Land Operations, Edition B, Version 1. Brussels: North Atlantic Treaty Organization.

- NATO (2022) NATO Strategic Concept. Brussels: North Atlantic Treaty Organization.

- NATO (2023) Climate Change and Security Agenda. Brussels: North Atlantic Treaty Organization. Available at: https://www.nato.int/cps/en/natolive/topics_82702.htm

- NATO (2023) NATO's Support to Ukraine. Brussels: North Atlantic Treaty Organization. Available at: https://www.nato.int/cps/en/natohq/topics_185520.htm

- NATO (2023) Security Force Assistance. Brussels: North Atlantic Treaty Organization.

- NATO (2024) Climate Change and Security Impact Assessment. Brussels: North Atlantic Treaty Organization. Available at:

https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/240709-Climate-Security-Impact.pdf

- NATO (2024) Emerging and Disruptive Technologies. Brussels: North Atlantic Treaty Organization. Available at: https://www.nato.int/cps/en/natohq/topics_184303.htm

- NATO (2025). "NATO Mission Iraq." NATO, Brussels. https://www.nato.int/cps/en/natohq/topics_166936.htm

- NATO (2024) NATO Releases Revised AI Strategy. Brussels: North Atlantic Treaty Organization. Available at: https://www.nato.int/cps/en/natohq/official_texts/227237.htm

- NATO (2025) Allied Joint Publication (AJP)-3.16: Allied Joint Doctrine for Security Force Assistance. Brussels: North Atlantic Treaty Organization. Edition B, Version 1, 2025.

- NATO Allied Command Transformation (2021) NATO Warfighting Capstone Concept (NWCC). Norfolk, VA: Allied Command Transformation. Available at: https://www.act.nato.int/wp-content/uploads/2023/09/nwcc_booklet.pdf

- NATO Allied Command Transformation (2023) ACT's 2023 Space Activities Recap. Norfolk, VA: Allied Command Transformation. Available at: https://www.act.nato.int/article/acts-2023-space-activities-recap

- NATO Allied Command Transformation (2023) Multi-Domain Operations: Enabling NATO to Out-Pace and Out-Think Its Adversaries. Norfolk, VA: Allied Command Transformation. Available at: https://www.act.nato.int/articles/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries

- NATO Allied Command Transformation (2023) Multi-Domain Operations Explained. Norfolk, VA: Allied Command Transformation. Available at: https://www.act.nato.int/activities/multi-domain-operations/

- NATO Allied Command Transformation (n.d.) NATO's Approach to Space. Norfolk, VA: Allied Command Transformation. Available at: https://www.act.nato.int/our-work/network-community/natos-approach-to-space/

- NATO Allied Command Transformation. Space: NATO's Newest Centre of Excellence. Norfolk, VA: Allied Command Transformation. Available at: https://www.act.nato.int/article/space-newest-coe

- NATO Communications and Information Agency (NCIA) (2024) NATO and Emerging Technologies. Brussels: NATO.

- NATO Defence Against Terrorism Centre of Excellence. Countering Hybrid Threats. Ankara: NATO. Available at: https://www.coedat.nato.int/

- NATO Rapid Deployable Corps Italy (NRDC-ITA) (n.d.) NATO Space Centre. Solbiate Olona: NATO Rapid Deployable Corps Italy. Available at: https://nrdc-ita.nato.int/nato-allied-reaction-force/component-commands/nato-space-centre

- NATO Science and Technology Organization (2024) Human Security – Frameworks, Concepts, Actors, and Challenges in Relevance to NATO. STO-TR-HFM-ET-201. Brussels: NATO Science and Technology Organization. Available at: https://www.sto.nato.int/

- NATO Security Force Assistance Centre of Excellence (2024) Remote Security Force Assistance: Reach Back Capability. Available at: https://www.nsfacoe.org/wp-content/uploads/2024/09/REMOTE-SFA-Reach-Back-Capabilities-Analysis-Report.pdf

- NATO Strategic Communications Centre of Excellence (2023) Artificial Intelligence and Influence Operations. Riga: NATO StratCom COE.

- North Atlantic Council (2021) NATO Climate Change and Security Action Plan. Brussels: NATO.

- North Atlantic Council (2021) Statement by the North Atlantic Council on the Recent Anti-Satellite Missile Test Conducted by the Russian Federation. Brussels: NATO. Available at: https://www.nato.int/cps/en/natohq/news_188780.htm

- Norwegian Centre for Research and Security Studies (NORSAR) (2023) GNSS Interference and Maritime Security Monitoring. Kjeller: NORSAR.

- Pérez, V., Aybar, C. and Pavía, J.M. (2024) 'Expanding the New Roles of the Military, The Case of Spain's Military Emergency Unit: A Research Note', Armed Forces & Society.

- Reuters (2025) NATO Scrambles Drones That Can Survive Arctic Conditions. Available at: https://www.reuters.com/world/nato-scrambles-drones-that-can-survive-arctic-2025-01-30/

- Royal Air Force (2025) Sky is No Longer the Limit for UK-US Military Operations. London: Royal Air Force. Available at: https://www.raf.mod.uk/news/articles/sky-is-no-longer-the-limit-for-uk-us-military-operations/

- Royal United Services Institute (RUSI) (2024) Lessons from the Maritime War in Ukraine. London: Royal United Services Institute.

- Royal United Services Institute (RUSI) (2024) Ukraine's Maritime Innovation: Lessons for NATO. London: Royal United Services Institute.

- Schaik, L. van et al. (2020) Ready for Take-off?: Military Responses to Climate Change. The Hague: Clingendael Institute.

- Skevaki, C. et al. (2024) 'Impact of Climate Change on Immune Responses and Barrier Defence', Journal of Allergy and Clinical Immunology. Available at: https://doi.org/10.1016/j.jaci.2024.01.016

- Space Force (2022) United States Space Force and Security Force Assistance: Standing Up the Regional Space Advisor Program. SFA Quarterly, 24th Edition.

- SpaceNews (2025) US Halts Satellite Imagery Support to Ukraine in Major Policy Shift. Washington, DC: SpaceNews. Available at: https://spacenews.com/us-halts-satellite-imagery-support-to-ukraine-in-major-policy-shift

- Swedish Police Authority (2022) Preliminary Investigation into the Nord Stream Explosions. Stockholm: Swedish Police Authority.

- Swedish Prosecutor's Office (2022) Statement on the Nord Stream Investigation. Stockholm: Swedish Prosecutor's Office.

- Tele Geography (2023) Submarine Cable Almanac. Washington, DC: Tele Geography.

- United Nations (1967) Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. New York: United Nations Office for Outer Space Affairs. Available at: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

- United Nations Conference on Trade and Development (UNCTAD) (2023) Review of Maritime Transport 2023. Geneva: United Nations. Available at: https://unctad.org/publication/review-maritime-transport-2023

- UNDP, 2022, United Nations Development Programme (2022). "Funding Facility for Stabilization – Iraq: Annual Report 2022."

- United Nations Security Council (2011) Resolution 2018 (2011) on Piracy and Armed Robbery at Sea. New York: United Nations.

- United Nations Security Council (2012) Resolution 2039 (2012) on Piracy and Armed Robbery at Sea. New York: United Nations.

- United States Naval Forces Africa (2007) Africa Partnership Station Programme. Naples: U.S. Naval Forces Africa.

- United States Space Force (2023) Space Force Instruction SPFI16-116: Regional Space Advisor Program. Available at: https://static.e-publishing.af.mil/production/1/ussf_csro/publication/spfi16-116/spfi16-116.pdf

- U.S. Department of Defense (2021) DOD, Navy Confront Climate Change Challenges in Southern Virginia. Washington, DC: Department of Defense.

- U.S. Department of Defense Office of Inspector General (2022) Special Report: Lessons Learned from Security Cooperation Activities in Afghanistan. Alexandria, VA: Department of Defense

Office of Inspector General. Available at: https://www.dodig.mil/reports.html/Article/3177119/special-report-lessons-learned-from-security-cooperation-activities-in-afghanis/

- U.S. Space Force (2023) Space Force Instruction SPFI16-116: Regional Space Advisor Program. Available at: https://static.e-publishing.af.mil/production/1/ussf_csro/publication/spfi16-116/spfi16-116.pdf

- U.S. Space Force (2025) US Space Force Unveils International Partnership Strategy to Strengthen Space Security. Available at: https://www.spaceforce.mil/News/Article-Display/Article/4234434/us-space-force-unveils-international-partnership-strategy-to-strengthen-space-s/

- White House (2023) Fact Sheet: Strengthening U.S. International Space Partnerships. Washington, DC: The White House. Available at: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/12/20/fact-sheet-strengthening-u-s-international-space-partnerships/

List of Abbreviations

A2/AD	Anti-Access/Area Denial
AC/135	Allied Committee 135 (NATO Codification System)
ACO	Allied Command Operations
ACT	Allied Command Transformation
AFSC	Alliance Future Surveillance and Control
AI	Artificial Intelligence
AIDA	Special Committee on Artificial Intelligence in a Digital Age (European Parliament)
AIRCOM	Allied Air Command
AIS	Automatic Identification System
AJOD	Allied Joint Operations Doctrine
AJP	Allied Joint Publication
APSS	Alliance Persistent Surveillance from Space
ASAT	Anti-Satellite (weapon)
AWACS	Airborne Warning and Control System
BAOS	Air Brigade of Space Operation
BI	Building Integrity
BICES	Battlefield Information Collection and Exploitation Systems

BIP	Building Integrity Programme
C2	Command and Control
C3OS	Space Operations Command and Control Center
C4	Command, Control, Communications and Computers
C5ISR	Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance
CAP	Comprehensive Assistance Package
CCASCOE	NATO Climate Change and Security Centre of Excellence
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CCW	Convention on Certain Conventional Weapons (UN)
CD&E	Concept Development and Experimentation
CDE	Commandement de l'Espace (French Space Command)
CERES	Capacité de Renseignement Électromagnétique Spatiale (French ELINT satellite system)
CERT-EU	Computer Emergency Response Team of the European Union
CFI	Civil Factor Integration

CFSPCC:	Combined Force Space Component Command
CI	Critical Infrastructure
C-IED	Countering Improvised Explosive Devices
CIICS	Cyber Information and Incident Coordination System
CIMIC	Civil-Military Cooperation
CIS	Communication and Information Systems
CMI	Civil-Military Interaction
CMOS	The Military Satellite Observation Center
CMX	Crisis Management Exercise
COA	Course of Action
COE	Centre of Excellence
COM NMI	Commander, NATO Mission Iraq
COPD	Comprehensive Operations Planning Directive
COSMOS	Centre Opérationnel de Surveillance Militaire des Objets Spatiaux
CRA	Cyber Resilience Act (EU)
CSIS	Center for Strategic and International Studies
CWIX	Coalition Warrior Interoperability Exercise
DA-ASAT	Direct Ascent Anti-Satellite (weapon)
DARPA	Defense Advanced Research Projects Agency (US)
DCAF	Geneva Centre for Security Sector Governance

DCB	Defence and Related Security Capacity Building
DEEP	Defence Education Enhancement Programme
DIANA	Defence Innovation Accelerator for the North Atlantic
DMAIC	Define, Measure, Analyze, Improve, Control
DoD	Department of Defense (US)
DOTMLPFI	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability
DTIS	Digital Transformation Implementation Strategy (NATO)
DUFMS	Defence University for Military Studies (Iraq)
ECDC	Education Cadre Development Centre (Iraq)
EDA	European Defence Agency
EDT	Emerging and Disruptive Technologies
ELINT	Electronic Intelligence
EO	Earth Observation
EOD	Explosive Ordnance Disposal
EU	European Union
EUAM Iraq	European Union Advisory Mission in Iraq
EUDIS	EU Defence Innovation Scheme

EUMAM Ukraine	EU Military Assistance Mission in support of Ukraine
EUNAVFOR	European Union Naval Force
EUSPA	European Union Agency for the Space Programme
EW	Electronic Warfare
FoN	Freedom of Navigation
FSF	Foreign Security Forces
FVEY	Five Eyes
GHG	Greenhouse Gas
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HANE	High Altitude Nuclear Explosion
HAPS	High-Altitude Pseudo-Satellite
HQ	Headquarters
HN	Host Nation
HR/IHL	Human Rights / International Humanitarian Law
Hum Sec	Human Security
IHL	International Humanitarian Law
IMMS	Iraqi Military Medical School
IO	International Organization
IoT	Internet of Things
IPCC	Intergovernmental Panel on Climate Change

ISO	International Organization for Standardization
ISR	Intelligence, Surveillance and Reconnaissance
JAIC	Joint Artificial Intelligence Center (US)
JAPCC	Joint Air Power Competence Centre
JCISFA	Joint Center for International Security Force Assistance (US)
JTEC	Joint Training and Evaluation Center (Georgia)
KLA	Kosovo Liberation Army
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LAWS	Lethal Autonomous Weapons Systems
LEO	Low Earth Orbit
LTO	Long-Term Objective
MAD	Ministerial Advisory Division (NMI)
MARSEC COE	NATO Maritime Security Centre of Excellence
MC	Military Committee (NATO)
MCDC	Multinational Capability Development Campaign
MCT	Maritime Counter-Terrorism
MDO	Multi-Domain Operations
MENA	Middle East and North Africa
METOC	Meteorological and Oceanographic (data and services)

MDFD	Multi-Domain Force Development
MIO	Maritime Interdiction Operations
MISP	Malware Information Sharing Platform
MoD	Ministry of Defence
MoI	Ministry of Interior
MOU	Memorandum of Understanding
MSA	Maritime Situational Awareness
MSO	Maritime Security Operations
MTI	Moving Target Indication
NATO	North Atlantic Treaty Organization
NCI Academy	NATO Communications and Information Academy
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NCSC	NATO Cyber Security Centre
NGO	Non-Governmental Organization
NISRF	NATO Intelligence, Surveillance and Reconnaissance Force
NLO	NATO Liaison Office
NMI	NATO Mission Iraq
NSpOC	NATO Space Operations Centre
NWCC	NATO Warfighting Capstone Concept

OECD	Organisation for Economic Co-operation and Development
ONSA	Office of the National Security Advisor (Iraq)
OOD	Operation Olympic Defender
OPLAN	Operation Plan
OSCE	Organization for Security and Co-operation in Europe
PDP	Professional Development Programme
PESCO	Permanent Structured Cooperation (EU)
PfP	Partnership for Peace
PID	Project Initiating Document
PM²	Project Management Methodology of the European Commission
PMBOK	Project Management Body of Knowledge
PME	Professional Military Education
PMNOC	Prime Minister National Operations Center (Iraq)
PN	Partner Nation
PNT	Positioning, Navigation and Timing
PRINCE2	Projects IN Controlled Environments
PRUs	Principles of Responsible Use (of Artificial Intelligence)
PSE	Professional Security Education Division (NMI)

RACI	Responsible, Accountable, Consulted, Informed
RF	Radio Frequency
RMP	Recognised Maritime Picture
RPO	Rendezvous Proximity Operation
RSA	Regional Space Advisor (Program)
RUSI	Royal United Services Institute
S5P	Global Partnership Directorate (US Space Force)
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SCRO	StratCom, Representation and Outreach Office (NMI)
SDA	Space Domain Awareness
SEAD	Suppression of Enemy Air Defences
SEI	Special Experience Identifier
SEW	Space Early Warning
SFA	Security Force Assistance
SFAB	Security Force Assistance Brigade (US Army)
SHAEF	Supreme Headquarters Allied Expeditionary Force
SHAPE	Supreme Headquarters Allied Powers Europe
SIGINT	Signals Intelligence
SLOC	Sea Lines of Communication

SME	Subject Matter Expert
SNGP	Substantial NATO-Georgia Package
SPCB	Specialised Programmes Coordination Branch (NMI)
SPS	Science for Peace and Security (Programme)
SSA	Space Situational Awareness
SSG	Security Sector Governance
SSR	Security Sector Reform
STANAG	Standardization Agreement (NATO)
STARCOM	Space Training and Readiness Command (US Space Force)
StratCom	Strategic Communications
TCCC	Tactical Combat Casualty Care
TDD	Training Development Division (NMI)
TTP	Tactics, Techniques and Procedures
UAP	Unified Action Partners
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UMS	Unmanned Maritime Systems
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea

UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNSCR	United Nations Security Council Resolution
USSF	United States Space Force
USV	Unmanned Surface Vessel
UUV	Unmanned Underwater Vehicle
UxS	Unmanned and Autonomous Systems
WMD	Weapons of Mass Destruction
WPS	Women, Peace and Security

NATO SECURITY FORCE ASSISTANCE CENTRE OF EXCELLENCE

"NATO's Multi-Domain Operations promise advantage through the speed and coherence with which effects are integrated across land, maritime, air, space, and cyberspace. Yet the Alliance rarely operates alone: its effectiveness is exercised through, alongside, and on behalf of partner nations. This Research Paper argues that Security Force Assistance is not a supplementary activity at the margins of MDO, but a structural enabler of it. Drawing on the contributions of seven Centres of Excellence, the operational insight of NATO Mission Iraq, and the perspective of civilian stakeholders, it examines how SFA must adapt — in doctrine, in resourcing, and in the metrics of success — to build partners capable of acting with the Alliance across every domain."

www.nsfacoe.org

9 788894 641561