# Adapting NATO's Counter-Terrorism Approach in a Multi-Domain Operational Context

## Workshop Report

**Emrah ÖZDEMİR**
**Editor**

**Ankara – Türkiye**
**2025**

# Adapting NATO's Counter-Terrorism Approach in a Multi-Domain Operational Context

## Workshop Report

**Emrah Özdemir**
**Editor**

**Ankara – Türkiye**
**2025**

# Adapting NATO's Counter-Terrorism Approach in a Multi-Domain Operational Context

**Workshop Report**

**16-17 September 2025**

**COE DAT**

**Ankara – TÜRKİYE**

**Emrah ÖZDEMİR**

Assoc. Prof. Academic Adviser and Editor

**LTC. Dietrich Klaus JENSCH**

Workshop Director

**Müge MEMİŞOĞLU AKAR**

Workshop Co-Director

**Elif Merve DUMANKAYA**

Rapporteur

**Derya DEĞER ÇEKİÇ**

Rapporteur



**Centre of Excellence**
**Defence Against Terrorism**

115 pages.
ISBN: 978-625-00-6438-2

**Address: Devlet Mahallesi İnönü Bulvarı Süleyman Emin Caddesi No:65 Çankaya 06582 Ankara, Türkiye**
**P.O. Box: P.K.- 57 06582 Bakanlıklar-Ankara, Türkiye Phone: +90 312 425 82 15 Fax: +90 312 425 64 89 E-mail: info@coedat.nato.int**

**DISCLAIMER**

This workshop report is a product of the Centre of Excellence Defence Against Terrorism (COE-DAT), and is produced for NATO, NATO member countries, NATO partners and related private and public institutions. The information and views expressed in this report are solely those of the authors and do not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the authors are affiliated.

**Content**

## At a Glance

### Core Message

- Despite increasing conventional threats and challenges, terrorism remains among NATO's most persistent asymmetric threats.
- Integration of Counter-Terrorism (CT) into Multi-Domain Operations (MDO) is essential to Alliance deterrence, resilience, and credibility.

### Threat Landscape

- Terrorists exploit drones, AI, cyber tools, and online radicalization for strategic impact, challenging NATO's MDO posture.
- Critical infrastructure and digital networks are primary targets, making resilience and cross-domain protection essential.
- Hybrid terrorism, often sustained by criminal networks or state sponsors, adds complexity to NATO's integrated multi-domain deterrence and defence efforts.
- Regional instability (Middle East, South Asia, Africa) fuels religiously motivated terrorism; far-right extremism grows within Allied societies, creating vulnerabilities across physical, cyber, and cognitive domains.

### Three Imperatives

1. Technological Convergence: Integrate counter-drone systems, AI-enabled intelligence, biometrics, secure communications, and predictive analytics across all operational domains to maintain NATO's technological edge.
2. Resilience and Adaptability: Embed counter-terrorism (CT) measures throughout land, air, maritime, cyber, and space domains; protect critical infrastructure; reinforce civil–military cooperation; and build societal resilience to withstand multi-domain shocks.
3. Strategic Agility: Update legal and policy frameworks to enable rapid, interoperable responses; institutionalise multi-domain coordination; and deepen NATO–EU–UN collaboration alongside structured public–private partnerships for cross-domain security.

### Education & Training

- Multipliers of resilience: scenario-based exercises, synthetic simulations, foresight-driven wargames, and cross-domain staff training to prepare forces for integrated multi-domain challenges.
- National models (e.g., Türkiye's integrated officer education reforms) illustrate best practice for embedding multi-domain thinking into professional military education.
- Priority: cultivate leaders with cognitive agility and decision-making skills to confront hybrid, multi-domain terrorism and operate effectively across land, air, maritime, cyber, and space domains.

**Conclusion**

- CT and MDO are converging realities rather than parallel tracks.
- Failure to integrate CT into the MDO framework risks strategic surprise and operational vulnerability.
- NATO's credibility and deterrence depend on strategic foresight, technological superiority, resilient societies, and adaptive education systems capable of preparing leaders for multi-domain challenges

# Executive Summary

The workshop *"Adapting NATO's Counter-Terrorism Approach in a Multi-Domain Operational Context"* (Ankara, 2025) underlined a critical point: terrorism remains one of NATO's most persistent asymmetric threats, and its integration into the Alliance's Multi-Domain Operations (MDO) framework is not optional but rather essential to the Alliance's strategic coherence.

Discussions confirmed that terrorist organizations are rapidly adapting. They exploit drones, artificial intelligence, and cyber tools to create strategic effects with limited resources. Critical infrastructure and digital networks are prime targets, while the acceleration of online radicalization fuels lone-actor and small-cell attacks that leave almost no warning. Hybrid terrorism—sustained by criminal networks and, in some cases, hostile states—adds further complexity. Although no large-scale biological or chemical attack has occurred, scientific advances demand preparedness.

Regional developments intensify this landscape. Fragile states in the Middle East, South Asia, and Africa remain hotbeds of religiously motivated violence, while far-right extremism grows within Western democracies. Terrorism is therefore not only an external challenge but a domestic and transnational one that undermines cohesion and trust in governments.

Three imperatives were highlighted:

1. Technological Convergence – NATO must invest in counter-drone systems, AI-enabled monitoring, biometrics, and secure communications to offset terrorists' asymmetric innovation.
2. Resilience and Adaptability – The Alliance must strengthen resilience in doctrine and practice, ensure civil–military cooperation, and prepare for hybrid crises across domains.
3. Strategic Agility – Legal and policy frameworks must be adapted for rapid, interoperable responses, supported by closer NATO–EU–UN coordination and structured public–private partnerships.

A particular emphasis was placed on education and training. Counter-terrorism in the MDO era requires not only technological upgrades but also a transformation in how personnel are trained and educated. Scenario-based exercises, digital simulations, and foresight-driven staff rides were identified as essential to prepare officers for hybrid and multi-domain threats. National innovations—such as Türkiye's reforms under the National Defence University, which integrate counter-terrorism, counterinsurgency, and MDO into officer education—were highlighted as valuable models for the Alliance. These efforts demonstrate how education

systems can serve as multipliers, producing leaders with the cognitive flexibility and practical expertise to confront terrorism across all domains.

The workshop concluded that NATO must not treat counter-terrorism and MDO as parallel efforts. Adversaries already exploit multi-domain vulnerabilities. Failure to integrate CT into MDO risks leaving the Alliance exposed to strategic surprise. NATO's credibility and deterrence rest on confronting this challenge directly—with foresight, technological edge, resilient societies, and a forward-looking education system capable of shaping leaders for tomorrow's operational context.

# Introduction

*Assoc. Prof. Emrah ÖZDEMİR – Academic Adviser and Editor*

**Scenario: The Overlooked Threat** (*illustrative scenario based on foresight analysis*)

In 2028, as NATO concentrates on deterring peer and near-peer adversaries through large-scale multi-domain exercises on the eastern flank, a dispersed terrorist network such as Daesh-K exploits overlooked vulnerabilities. Coordinated attacks unfold across several Allied capitals:

- Cyber operations paralyse metropolitan transport systems, leaving millions stranded.
- Swarms of commercial drones release small explosives on public gatherings, generating fear disproportionate to their scale.
- Armed cells conduct simultaneous assaults in shopping districts, livestreamed on hijacked social media platforms.
- A cyber-attack on satellite navigation signals disrupts aviation, grounding flights and slowing emergency response.
- AI-generated disinformation spreads across the digital space, fuelling conspiracy theories and eroding public trust.

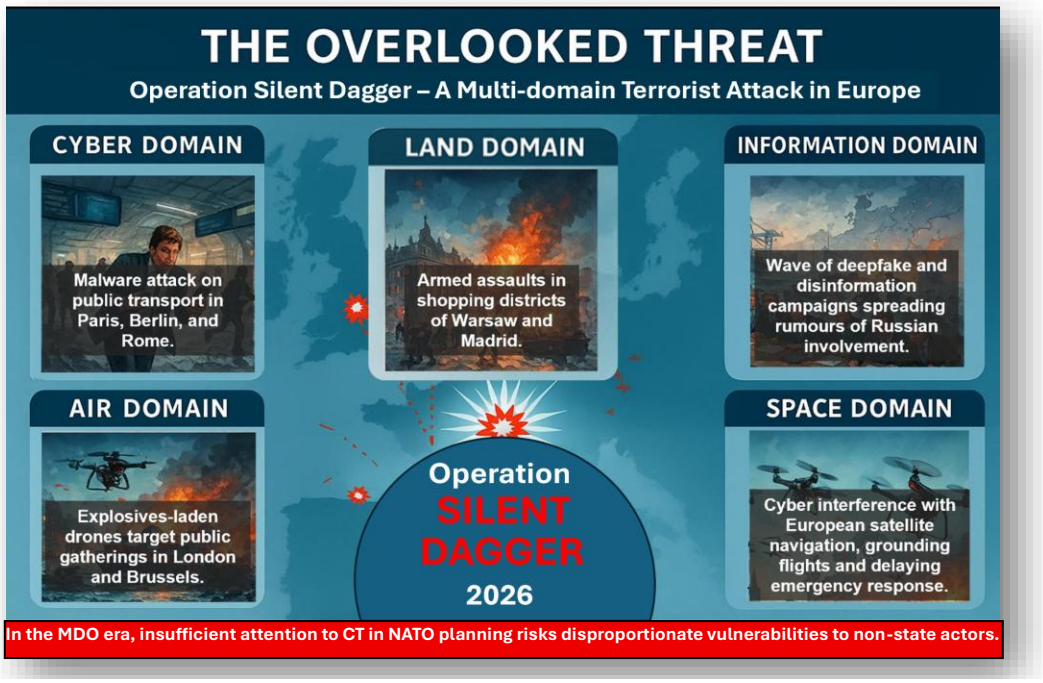



*Figure 1 Illustrative scenario based on foresight analysis.*

The immediate toll is tragic, but the wider effect is strategic shock. Critical infrastructure is paralysed, political cohesion is strained, and NATO is forced to confront the reality that while it prepared for multi-domain conflict with state adversaries, it underestimated the capacity of non-state actors to act across multiple domains.

This scenario highlights a core lesson: counter-terrorism is not a legacy task. In the multi-domain era, even dispersed terrorist groups can combine cyber, information, space, and physical attacks to challenge Allied resilience. Moreover, terrorist organisations may increasingly be employed as proxies or instruments by peer and near-peer adversaries to exploit vulnerabilities across multiple domains. Failure to address this risk as part of NATO's deterrence and defence posture leaves a critical blind spot open to exploitation.

**Context of the Workshop**

This scenario illustrates why counter-terrorism must be fully integrated into NATO's MDO Concept. Against this backdrop, the workshop *"Adapting NATO's Counter-Terrorism Approach in a Multi-Domain Operational Context"* (Ankara, 2025), convened in Ankara, addressed a key strategic challenge for the Alliance: how to ensure that NATO's counter-terrorism posture evolves in step with the adoption of MDO. As reaffirmed in the NATO 2022 Strategic Concept, terrorism remains "the most direct asymmetric threat" to Allied security. Today, terrorist actors increasingly operate in ways that mirror the dynamics of multi-domain conflict—integrating cyber and information warfare, leveraging emerging technologies, and conducting physical attacks against infrastructure and populations. In this respect, NATO's counter-terrorism efforts cannot be treated as peripheral but must be embedded in the Alliance's broader deterrence and defence posture.

**Rationale**

This rationale is anchored in NATO's foresight analyses and the outcomes of the Hague Summit 2025, both of which underline the adaptive capacity of non-state actors and the blurring boundaries between terrorism, hybrid threats, organized crime, and proxy warfare. Terrorist organizations now weaponize inexpensive commercial drones, employ artificial intelligence to amplify disinformation and cyberattacks, and exploit vulnerabilities in critical infrastructure. Their decentralised and resilient structures echo many of the challenges NATO anticipates in a contested multi-domain environment. If counter-terrorism is positioned as secondary to state-focused threats, NATO risks a strategic blind spot, undermining both deterrence credibility and the protection of Allied populations. By integrating counter-terrorism within the MDO framework, NATO aligns its doctrine and capabilities with the evolving threat landscape and reaffirms its collective resilience.

**Workshop Objectives and Design**

Building on this strategic foundation, the workshop was designed with three interlinked objectives:

1. **Assess NATO's current counter-terrorism approach** in the context of multi-domain threats, including how terrorism intersects with cyber, space, information, and the electromagnetic spectrum alongside the physical domains, and evaluate its alignment with NATO's MDO concept.

2. **Identify doctrinal, capability, and operational** gaps that hinder the integration of counter-terrorism into MDO, in line with NATO's Foresight Analysis which highlights the convergence of state and non-state threats across multiple domains.

3. **Collaborate to develop actionable recommendations** for embedding counter-terrorism into NATO's MDO posture—spanning policy alignment, capability development, and training design—consistent with COE-DAT's mandate to drive innovation and interoperability in multi-domain counter-terrorism.

To achieve these objectives, the first day of the workshop was conceived as a preliminary session to establish a shared understanding among all participants and create a strong common baseline before moving into group work. This session concentrated on strategic foresight, NATO's current CT posture, future warfare trends, the integration of CT into MDO, and planning an up-to-date training system. Expert contributions ensured not only the provision of analytical insights but also the creation of a shared framework for subsequent discussions.

**Methodology: A Focus Group Approach**

In line with NATO's emphasis on innovation, education, and civil-military engagement, the workshop was structured around a focus group interview methodology. This format moved beyond traditional presentations to foster structured interaction among participants from diverse professional communities—military officers, law-enforcement officer, policy-makers, and academics. The approach generated insights that:

- Tested assumptions about the adaptability of MDO concepts to counter-terrorism;
- Examined practical cases of hybrid terrorism and their doctrinal implications;
- Encouraged exchange between practitioners and scholars on training, education, and capability development;
- Produced recommendations grounded in both operational feasibility and strategic foresight.

On the second day, the workshop shifted from vision to practice. **Group 1** addressed doctrinal adaptation, while **Group 2** examined capability and training enhancements. Together,

their work formed the backbone of the final recommendations for aligning NATO's counter-terrorism approach with the evolving realities of multi-domain operations.

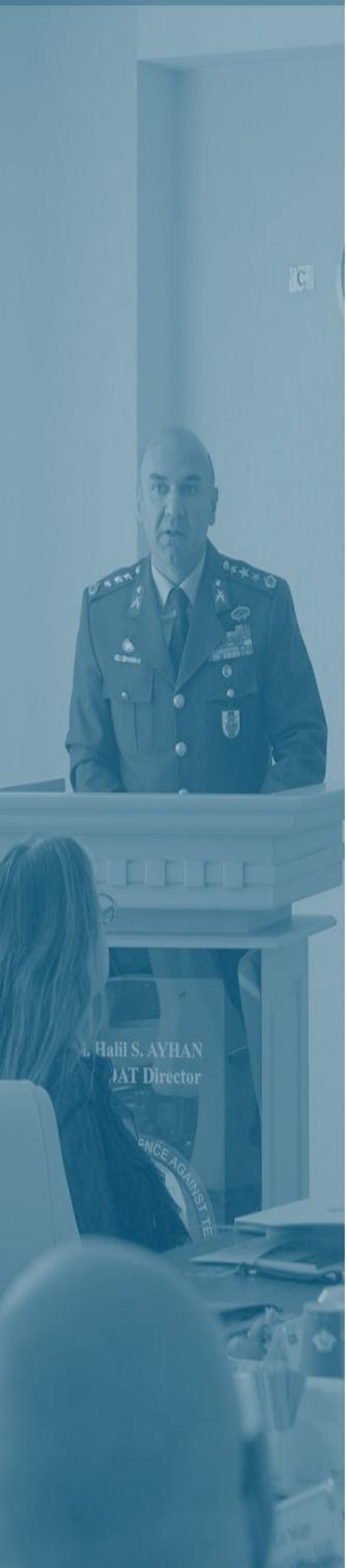
This interactive format encouraged candid dialogue, illuminating areas of consensus and tension alike, and ensured that the workshop outcomes are not only forward-looking but also actionable, in line with NATO's culture of continuous adaptation.

**Scope and Key Takeaways**

The workshop was not intended to provide exhaustive policy prescriptions but rather to generate a shared baseline and insights consistent with NATO's foresight and strategic planning. After two days of intensive dialogue, several clear messages emerged: counter-terrorism must be fully integrated into NATO's MDO approach; doctrine and capabilities need to adapt with greater unity and agility across all domains; training and education systems must reflect the realities of hybrid and multi-domain terrorism; and foresight and technology will be decisive in ensuring resilience and interoperability. These key takeaways will guide the more detailed recommendations presented in the concluding section of this report.

**Report Structure**

This report is structured to reflect the progression of the workshop itself. The first section captures the preliminary sessions, which provided expert presentations and analytical framing on NATO's current counter-terrorism posture, multi-domain challenges, and future warfare trends. The second section presents the discussions of the two working groups: Group 1 on doctrinal adaptation and Group 2 on capability and training enhancements. The final section consolidates these insights into an overarching discussion, highlighting the main takeaways and recommendations that emerged from the workshop**.**




# Opening Remarks

# Opening Remarks of the COEDAT Director


Ladies and Gentlemen, Dear Colleagues,

It is my great pleasure to welcome you to our workshop "Adapting NATO's Counter-Terrorism Strategy in the Context of Multi-Domain Operations." I am delighted to see so many experts from research, the military, politics, and practice gathered here today, and I would like to sincerely thank you all for participating in this workshop. Also, I would like to offer a warm welcome to our Academic Advisor Assoc. Prof. Emrah ÖZDEMİR. We are grateful for his expertise and advice, which was instrumental in the planning of this event. Before proceeding, I would like to extend my deepest appreciation to Major General Eray ÜNGÜDER Director of Cooperative Security Division for his continuous support. I would also like to acknowledge with gratitude the valuable contributions of Transformation Dept. staff; Capt. Hakan GÖMENGİL, Ltc Dietrich Klaus JENSCH and Mrs Müge MEMİŞOĞLU AKAR in making this workshop possible.

The threat of terrorism, unfortunately, is not a phenomenon of the past. It continues to evolve, adapts to new technologies, and exploits vulnerabilities in our societies, in our structures, and even in our armed forces. While in past decades our focus was primarily on more traditional forms of terrorism, today we face a far more complex environment: terrorist actors are no longer operating only in the physical space but increasingly in cyberspace, in the information domain, and across hybrid grey zones.

This is precisely where the concept of Multi-Domain Operations comes into play. By no longer viewing defence and security in isolation, but instead integrating efforts across land, air, sea, space, and cyber, we can significantly enhance our counter-terrorism strategies. The key question is how NATO members can pool their capabilities, their information, and their resources to remain operational across all domains simultaneously.

CT is a part of this, and this workshop is intended to be the starting point for exploring how and where CT is, or should be, integrated into the overall MDO concept. Based on the previous review of the development of MDO concepts and ideas, COEDAT believes that CT should not be neglected.

Our workshop today offers the opportunity to discuss this challenge together:

- Which elements of the existing NATO strategy are changing?
- Where do we need to adapt or even completely rethink our approach?

• And how can we use innovation, technology, and international cooperation to prepare for future threats?

I invite all of you to engage openly, critically, and creatively in today's discussions. What we need are not only technical or military answers, but also political and societal perspectives.

Thank you very much for being here, for sharing your expertise, and for your willingness to work together on this topic. Let us use this time to generate impulses that will resonate beyond this workshop and remain effective in the realities of tomorrow.

Thank you – and I wish us all a productive and inspiring exchange.

Halil Sıddık AYHAN
Colonel, TÜR A
Director

## Future Trends in Terrorism

*LTC. Dietrich Klaus JENSCH – Workshop Director*

Expect the unexpected—a fundamental tactical principle that holds particular relevance in the field of counter-terrorism.

One of the goals of the workshop is to keep up to date with developments in the field of Multi-Domain Operations and to shed light on their future orientation not only in the area of classical/modern warfare, but also with regard to T/CT.

Besides the main topic, the aim of this workshop is also to consider a future direction for counter-terrorism within an MDO-based command and control system and to develop scenarios. This cannot, of course, be achieved in a single workshop; therefore, this workshop should only be the starting point.

In the future, MDO is expected to evolve beyond a conceptual framework into a foundational element of operational planning, integrating technology and training—particularly in environments involving state-level competitors. Alongside such conventional challenges, diverse forms of terrorism will persist. The timely recognition of these threats and their evolving tactics, as well as the ability to effectively counter them, remain critical challenges for NATO and its allied and partner forces.

The often-observed tendency to focus primarily on a current problem, currently the full-scale invasion of Ukraine, carries the risk of neglecting other threats and throwing the "overall situation picture" off balance.

The following developments are expected by 2040.

• Multi-domain operations will become the norm, not the exception: Every major operation will be planned, executed, monitored, and ultimately evaluated across domains.

• Competition between world powers below the threshold of open warfare will become more important—for example, cyberattacks, space confrontations, and influence operations.

• Gain speed in data processing and information superiority: through rapid networking, data supremacy, and precision.

• Alliance and partner operability: States and alliances must develop common standards, tactics, and networks – isolation is increasingly becoming a weakness.

All this takes place under the ever-present threat of terrorism, which we must always be aware of.

# Keynote Speech

# Future Counter-Terrorism in a Multi-Domain World

*Gabriele CASCONE – Head CT/OPS, NATO HQ*

To get us started, I would like to present you with two definitions.

Counter-terrorism, as defined in NATO is: All preventive, defensive and offensive measures taken to reduce the vulnerability of forces, individuals and property against terrorist threats and/or acts, and to respond to terrorist acts.

Multi-Domain Operations is: The orchestration of military activities, across all domains and environments, synchronised with non-military activities, to enable the Alliance to create converging effects at the speed of relevance.

I think that already we can see very tight links and complementarity between the two concepts – so that is good news for this conference!

Before delving into the linkages between NATO CT and MDO, let me review for you the origins of NATO Counter-terrorism.

NATO's approach to Counter-terrorism has evolved over time, adapting both the threat itself and to Allies' desire to use NATO as a tool to combat terrorism.

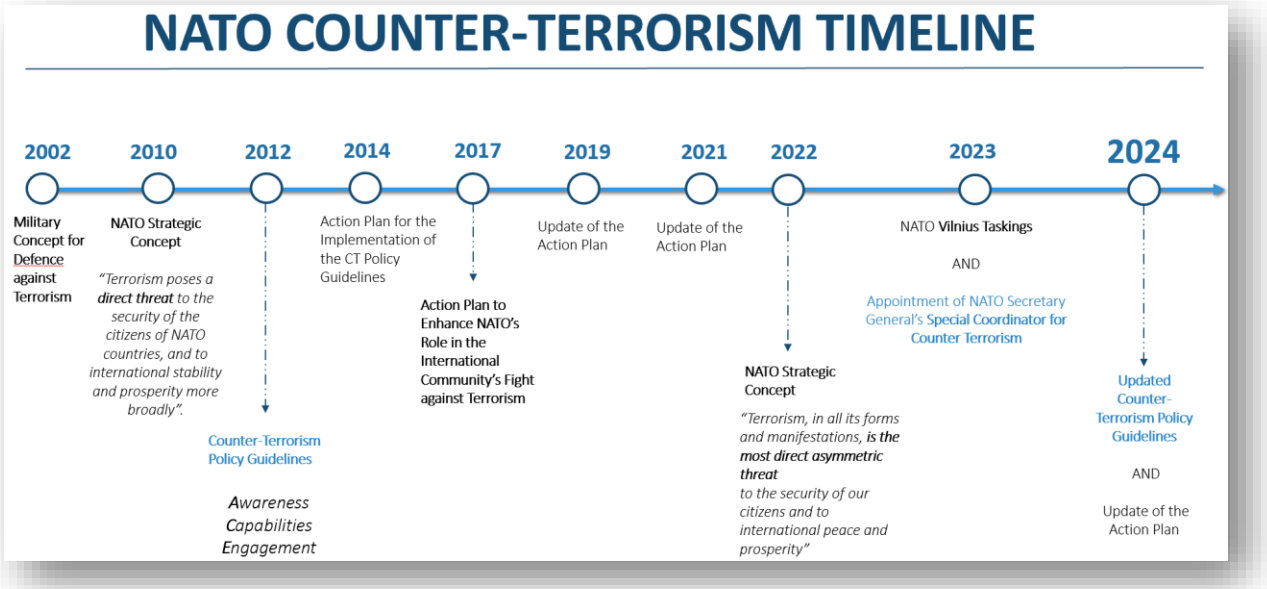



*Figure 2 NATO Counter-Terrorism Timeline*

Two big trends have been:

1. That since the 2010 Strategic Concept to the 2022 Strategic Concept, to the terrorist threat has been added the threat from Russia.

2. Since the end of the ISAF/RSM Operations, the focus of NATO work on CT has shifted from to awareness, capabilities and engagement with allies and partners.

Nonetheless, a through-line in this history of NATO CT is the comprehensive approach, the cooperation between military and civilian authorities and the continued unity of the Alliance in the face of the evolving threat.

At the Vilnius Summit in 2023, heads of state and government decided to update NATO's Counter-terrorism Policy Guidelines. Completed in 2024, these guidelines lay down the main principles under which the Alliance should contribute to the international fight against terrorism. The guidelines reaffirm our commitment to comply with international law, support Allies, and ensure non-duplication and complementarity.

In practical terms, these guidelines identified those areas where NATO can contribute to this international effort most efficiently, including:

(1) Improving our collective awareness of the terrorist threats,

(2) Ensuring that we have adequate capabilities and preparedness to respond in case of crisis and,

(3) Enhancing our engagement with other key players within this effort, whether individual partner countries, regional groupings and international organizations.

I provide here a slightly more granular look at the main areas of effort under the 2024 CT Action Plan:

- Increase situational awareness on terrorist groups;
- Leverage the use of technologies in the fight against terrorism;
- Further engagement with partners and other international organisations in the fight against terrorism.
- Exploration of a possible NATO role in countering the financing of terrorism (Cultural Property Protection a first promising strand of work).
- Continuation of ongoing work-strands**.**

So, from those last slides, I think it will be easy for this audience to see that there are many parallels between NATO's approach to Counter-terrorism and the Multi Domain Operations approach. Indeed, our approach to CT has been multi-domain all along. The NATO Concept for MDO is therefore a very useful addition to the conceptual framework in which we conduct NATO CT.

Before I go further into further detail about how MDO and CT dovetail conceptually and practically, I would like to share the following observations. While not really caveats, they do draw important distinctions between MDO and NATO's CT work:

- In the area of CT, it is especially important to underline that Nations retain the primary responsibility for their domestic security and their own resilience and thus for countering terrorism.
- NATO MDO is military focused and does not seek to replace the intent of a comprehensive approach. While NATO's CT work is ultimately in *support* to Allies, who have the primary responsibility to counter terrorism, NATO's MDO approach is fundamentally about making NATO work.
- Finally, I would observe that the fight against terrorism still demands a coherent, steady effort by NATO and the international community as a whole, involving a wide range of instruments and actors. This perhaps brings us full circle – as MDO also is very dependent on the aggregation of multiple instruments of power, both military and civilian.

Given the caveat that Nations retain the primary responsibility for CT and that MDO is above all military focused, I would like to share some thought and some examples of how NATO CT work contributes to and/or is enhanced by the various Enablers to MDO.

**Data**: MDO demands a data centric approach that recognizes data as a strategic asset

Under the umbrella of NATO CT, NATO has developed Battlefield Evidence, Biometrics and Technical Exploitation Policies that highlight the need for NATO to leverage *Battlefield Forensics* in the support of political and military decision making – much in the same way that forensics supports law enforcement in the civilian space. Data is, of course, central to these initiatives.

Two practical examples are:

1. We are exploring developing a Battlefield Evidence Data Exchange to enable the sharing of information collected by the military with civilian authorities to support civilian outcomes

2. The NATO Automated Biometrics Information System, a system to connect National biometrics databases based on a "ping-and-ring" system to enable the sharing of biometrics data for operational purposes while fully respecting international and national laws and policies regarding the sharing of personal information.

The Future CT in a Multi-Domain World will need to build on NATO-wide data initiatives to expand data sharing/exchange/appreciation/exploitation beyond these areas and to integrate battlefield forensics information into the broader NATO Intelligence Enterprise.

As you have seen, leveraging technology is already a key tenet of NATO's CT work, and the MDO concept only enhances that emphasis.

Under the NATO CT Action Plan, we emphasize integrating Emerging and Disruptive Technologies into CT capability development. We execute this under our NATO Defence Against Terrorism Programme of Work, where we have a long history of supporting multinational technology initiatives such as:

- integrating Artificial Intelligence into drone operations, decision making tools and sensor fusion operations

- exploring the application of innovative manufacturing techniques and smart materials into military hardware

- leveraging technology to augment human physical and mental performance, including decision making

- understanding both the threat and the opportunities presented by advances in bio-technology.

While most of this work is led by Nations, we encourage Incorporation of EDTs & Support to development of NATO Computer and Information Services in order to build and maintain the Alliance's technological edge.

MDO relies on collaborative, agile and empowered, multi-domain C2

This is an area in which we have not done a lot of work, for while essential to CT, it is not really in the lane of NATO's CT work - and quite honestly is a big challenge in NATO.

Nonetheless, the NATO Military Authorities are developing more agile cross-domain approach to C2 relationships, such as the Cross Domain Command Concept' and the 'Integrated Multi-Domain Architecture Concept.

In a future, multi-domain world, developing broader collaboration between military commanders and non-military actors in order to understand, utilise and synchronise capabilities that are not directly under NATO C2 will be an enormous, but necessary challenge.

My long experience in NATO has taught me that the Right People with the Right Skills are essential to getting anything done – so I'm very happy to see this spelled out so explicitly in NATO's MDO Concept.

Our NATO CT work has seen an increased involvement of NATO Military Authorities in CT Action Plan, despite the end of the ISAF/RSM operations.

There is important CT work being conducted by our colleagues in SHAPE and on the International Staff in the of Family of Plans.

One area that I will highlight here, is the role of Gendarmerie –type forces as MDO leaders. These types of forces, with their training and their authorities firmly established in both the military and civilian law enforcement worlds, can play an essential role as the glue between the "conventional" military forces and operations and those Non-Military Instruments of Power and stakeholders that are essential to fulfilling the Vision for an MDO-Enabled Alliance.

Finally, MDO needs investment in technologically enabled training at the national and NATO levels.

Traditionally, training is a national responsibility, but NATO can provide "over and above" training and exercise opportunities in order to enable an MDO force.

Examples from NATO CT have been

- Battlefield Evidence integration into Exercise TROJAN FOOTPRINT, where NATO concepts have supported bridging the gap between Special Forces and Civilian law enforcement in a hybrid scenario

- Biometrics integration into Exercise STEADFAST INTEREST – which is demonstrating the use of biometrics in support of military HUMINT, not just to identify "bad guys" but to also identify the innocents that often are swept up in storm of warfare – displaced persons, missing family members, etc. As we know from experience, in both conventional and counter-terrorism operations, maintaining the hearts and minds of the majority of the affected populations is critical to mission success.

- We also conduct CT training for NATO partners, so that by contributing to the stability and security of their own nations, NATO security is ensured.

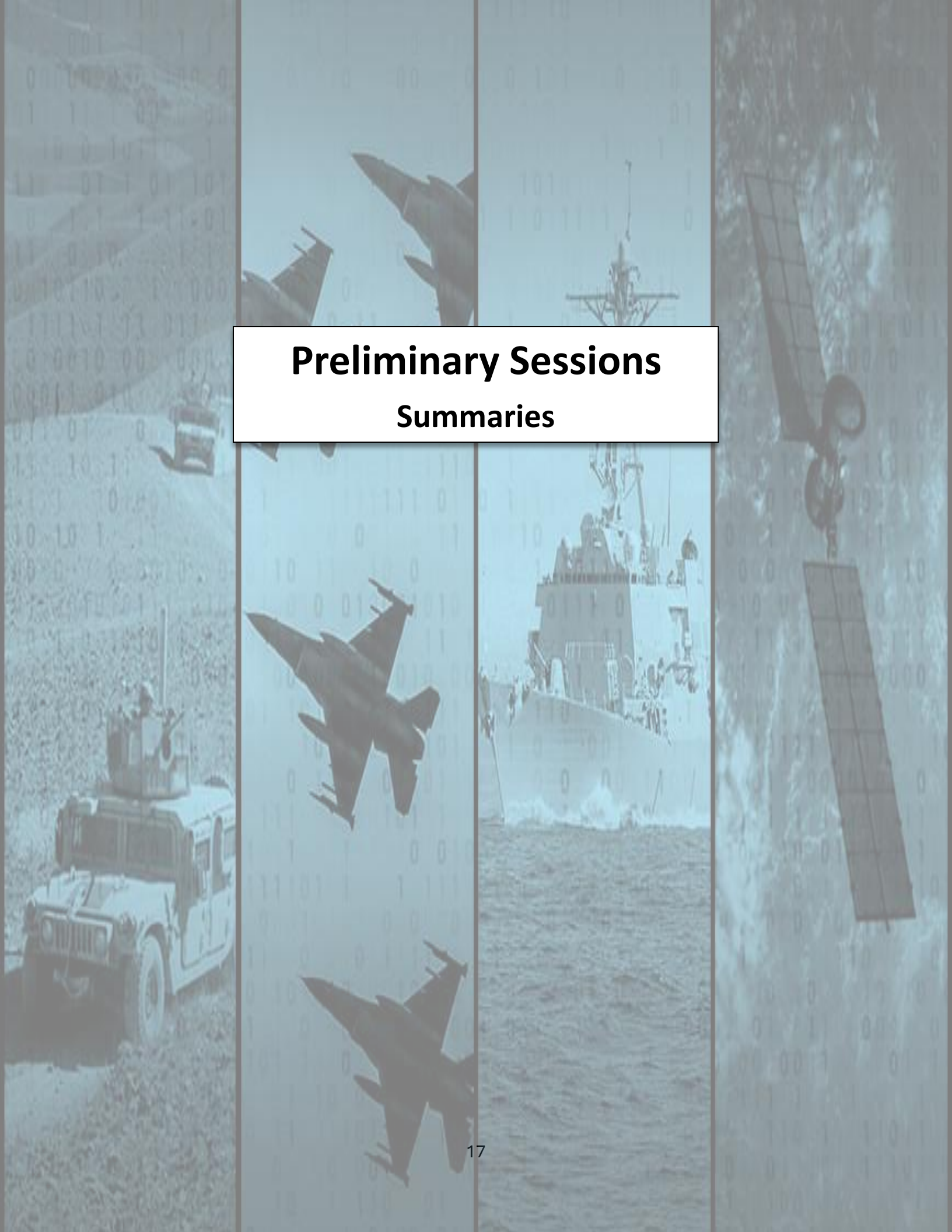
In a future Multi-Domain World, we will need to more consciously plan for Nations to provide "MDO-trained" personnel to NATO, where NATO "over and above" training can build on the nationally provided foundation.

In conclusion, I would like to stress the following aspects of MDO and how they relate to NATO Counter-terrorism:

1. As the definition of MDO says, MDO is about orchestrating Military activities, which are the purview of the Alliance, with non-military activities, that largely are not the purview of the Alliance. This is something that we in the Counter-terrorism community are very familiar with, because CT is primarily a National rather than a NATO responsibility and, for most Nations, CT is a civilian-led rather than a military led activity.

2. As recognized in NATO's MDO Concept, our adversaries are already multi-domain. Unfortunately, we in the NATO CT community are also familiar with the need for the Alliance to do some catching up to do in order to match our adversary's agility.

3. What we can learn from our experience of Counter-terrorism is that one of biggest strengths we have is Unity. The common values and rule of law that underpin the NATO Alliance provide us with a foundation that cannot be matched by our adversaries. And as with Counter-terrorism, this will also be foundation of the success for Multi-domain Operations.



# Preliminary Sessions

## Summaries

### *Session 1. Strategic Foresight & Evolving Threats*

- ***Key Insight:*** *Terrorism is evolving into a multidomain phenomenon, merging cyber, financial, and information tactics.*
- ***Policy Takeaway:*** *NATO must integrate CT into foresight planning, not treat it as a residual task.*
- ***Operational Implication:*** *Exercises should simulate hybrid campaigns blending cyber-attacks and disinformation.*
- ***Future Priority:*** *Develop a foresight cell dedicated to CT within MDO planning.*

# Foresight Analysis in the Context of MDO Strategies

*Oğuz KALAYCIOĞLU – Senior Enterprise Architect · ACT*

**Introduction**

Modern security environments are defined by volatility, uncertainty, complexity, and ambiguity. State and non-state actors alike employ rapid technological advances, cyber capabilities, information warfare, and hybrid tactics to challenge traditional defence constructs. In this environment, Multi-Domain Operations (MDO)—the integration of effects across land, sea, air, space, and cyberspace—have emerged as a dominant strategic paradigm. To sustain operational advantage within MDO, defence organizations must anticipate change rather than merely react to it. This is the central utility of foresight analysis: a structured process to anticipate emerging trends, explore alternative futures, and inform robust strategic decision-making.

**Defining Foresight Analysis**

Foresight analysis is not prediction; rather, it is a disciplined approach to exploring plausible futures and their implications. By combining trend scanning, horizon scanning, scenario building, and systems thinking, foresight enables leaders to prepare for a range of contingencies. It emphasizes early identification of weak signals—small indicators of larger shifts—that could disrupt operational concepts or create new opportunities. In the context of MDO, foresight analysis bridges strategic vision with technological and doctrinal development, ensuring that capabilities are aligned with potential futures rather than locked into outdated paradigms.


*Figure 3 Strategic Foresight Process*

**Foresight and the Multi-Domain Environment**

MDO requires seamless integration across domains traditionally managed in isolation. This integration heightens complexity: actions in cyberspace can trigger consequences in the physical domain, while space assets enable targeting and communication across all others. Foresight analysis allows military planners to map these interdependencies, identifying both vulnerabilities and leverage points.

For example, foresight methods might reveal how adversaries' investment in autonomous swarms could reshape the tempo of operations, forcing coalition forces to develop counter-swarms or electronic warfare tactics. Similarly, foresight can assess how the proliferation of commercial space assets will alter the contested space domain, offering both opportunities for data exploitation and risks of dependency on fragile infrastructures.

**Key Functions of Foresight in MDO Strategy**

1. **Trend Identification and Technology Watch**: Foresight analysis systematically tracks emerging technologies—artificial intelligence, quantum computing, hypersonic, directed energy, and resilient communications. In MDO, where technological surprise can shift balances rapidly, the ability to anticipate disruptive technologies is decisive.
2. **Scenario Development and Wargaming**: By constructing multiple future scenarios, foresight enables commanders to test strategies under varied conditions: peer-state conflict, gray-zone competition, or coalition stabilization operations. In wargaming, these scenarios highlight operational risks and help identify cross-domain synergies or gaps.
3. **Capability Development Alignment**: Foresight informs long-term investment decisions, ensuring that modernization programs reflect plausible future demands rather than solely current challenges. This reduces the risk of capability obsolescence and promotes adaptive force structures.
4. **Resilience and Adaptability**: MDO strategies rely on resilient networks, adaptable command structures, and flexible logistics. Foresight identifies potential system shocks—such as cyber intrusions, space asset denial, or contested logistics routes—and helps design **redundant, agile solutions**.

**Strategic Implications**

Incorporating foresight analysis into MDO planning offers several strategic benefits. First, it strengthens deterrence, as adversaries recognize that the force is prepared for a wide spectrum of futures. Second, it enhances coalition interoperability, since foresight-based planning fosters shared understanding of threats and opportunities among allies. Finally, foresight contributes to ethical and legal preparedness, as future scenarios can be used to anticipate dilemmas in areas such as autonomous weapons or information manipulation.

The future of MDO; “Mosaic Warfare” is a military concept that envisions breaking large, monolithic systems into smaller, adaptable, and interoperable components—like tiles in a mosaic—that can be rapidly combined, reconfigured, and deployed to achieve mission objectives with greater flexibility, resilience, and speed.

Mosaic Warfare, when examined through the lens of Foresight Analysis, represents a transformative shift in how future conflicts may unfold. Instead of relying on monolithic, platform-centric approaches, mosaic warfare emphasizes modular, interoperable, and rapidly reconfigurable systems that can be combined like tiles in a mosaic to achieve mission effects. From a foresight perspective, this approach anticipates a battlespace where adaptability, resilience, and distributed decision-making become decisive advantages in the face of uncertainty. By exploring alternative futures, scenario planning, and horizon scanning, foresight analysis can help identify the conditions under which mosaic warfare offers the greatest strategic utility, as well as the potential vulnerabilities—such as cyber dependencies, interoperability challenges, or adversarial counter-adaptation—that could limit its effectiveness. Ultimately, foresight-driven exploration of mosaic warfare enables defence planners to not only anticipate emerging risks but also shape investments and doctrines that leverage modularity and innovation to maintain strategic advantage in complex, evolving security environments.


**Challenges and Limitations**

Despite its advantages, foresight analysis in the MDO context faces challenges. Cognitive bias, institutional inertia, and resource competition can limit its influence on decision-making. Additionally, the sheer pace of technological change can overwhelm analytic capacity.

Therefore, foresight should not be seen as a one-time activity but as a continuous, iterative process embedded into strategic culture.

**Conclusion**

Foresight analysis is an indispensable tool for navigating the uncertainty of the multi-domain battlespace. By anticipating emerging trends, testing strategies against diverse scenarios, and aligning capabilities with possible futures, foresight empowers decision-makers to sustain advantage in complex security environments. Multi-Domain Operations demand not only integration of military power across domains but also integration of thinking across time horizons. In this respect, foresight analysis ensures that military organizations are not merely responsive to change but are proactive shapers of the future battlespace.

# Beyond Overmatch: Asymmetry and CT in the Era of MDO

*Dr. Roderick PARKES – NATO Defence College*

**Introduction**

This paper examines how NATO's concept of MDO and its CT policy might be better aligned by 2030. MDO envisions integrated effects across land, sea, air, space and cyberspace to maintain battlefield advantage. CT has been shaped by irregular threats, hybrid actors and complex civilian terrain. The question is whether MDO—developed with peer-state competition in mind—can adapt to the fluid, decentralised realities of countering terrorism, and how CT may need to adjust to the demands of multi-domain thinking already evident in state-backed terror.

The focus here is not operational or tactical detail—ground better covered by practitioners—but the assumptions behind each approach, and how they might pull apart over the next five years. The aim is to clarify where MDO and CT may leave gaps if left unaligned, and to suggest areas where doctrine or training could evolve to close them.

**Imagining how different drivers play out**

Strategic foresight does not lay out fixed paths for how terrorism will evolve or predict specific scenarios for how it might manifest. Instead, it asks how the same major drivers—such as technology, geopolitics or demographics—might combine in unexpected ways over time. By sketching several possible futures for terrorism and then "looking back" on today, we can test whether current thinking on MDO and CT rests on shaky assumptions or overlooks important factors.

These exploratory scenarios differ from disruptive "what if" exercises that imagine 9/11-style, high-impact, low-probability events. Such scenarios can be useful for preparing organisations for moments of stress, but they risk portraying terrorism as a series of isolated shocks rather than as the product of structural pressures and continual adaptation. They also tend to be rooted in weaknesses we already recognise, which limits their value.

**The five major drivers to 2030**

The decade ahead is already being shaped by a set of powerful trends highlighted in NATO's Allied Command Transformation foresight work to 2030.

- **Great-power competition** will remain the main organising force in international affairs. Rivalries among a few large states will draw political attention away from global

problems, drive proxy conflicts and territorial disputes, and influence how resources are allocated to counter-terrorism—indeed, what is considered terrorism and what coalitions form to combat it.

- **The state's traditional monopoly on force, capital and legitimacy** is weakening. Non-state actors can buy or build advanced weapons, move funds through cryptocurrencies, and spread messages instantly to global audiences. New state-like entities may also emerge beyond traditional borders and jurisdictions.
- **Norms, loyalties and identities** are in flux. Allegiances are shifting and contested, attribution is harder, and new cross-border or online loyalties are forming just as old grievances re-emerge. In this context, the struggle for narrative credibility can be as decisive as battlefield outcomes.
- **Environmental stress** is reshaping the operating environment. Melting ice, drought and extreme weather open new routes and resources but also make it harder to hold territory, sustain logistics or support populations—creating societal pressures and zones terrorists may exploit.
- **Technological change** is transforming the capabilities of both states and non-state actors. Artificial intelligence, autonomy, quantum tools and ubiquitous sensors are moving quickly into use. Terrorist groups can exploit commercial innovation—using drones, deepfakes or malware—at a fraction of the cost required for states to defend against them.

These drivers form the baseline conditions under which counter-terrorism will unfold. The uncertainty lies in how they interact, and the directions they may take.

**Exploring trajectories in a simple 2×2**

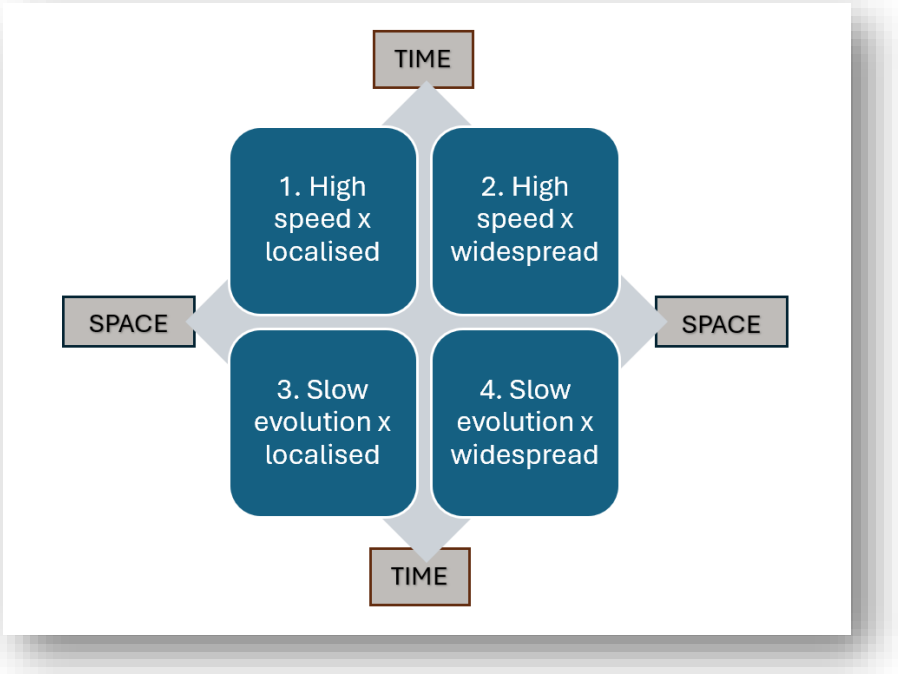
The trends described above can be assumed to play out in relatively predictable ways for MDO, which is built on the expectation of peer conflict and the ability to synchronise across domains and extended geographies—high-speed and widespread effects. For CT, such assumptions cannot be taken for granted. Terrorist activity is irregular, opportunistic and often shaped by local conditions, making its trajectory harder to plot.

To probe this uncertainty, we use a simple 2×2 framework. It is not intended to predict outcomes, but to test whether terrorism can be understood in the same terms as MDO. The two variables are:

**Time:** rapid and compressed versus slow and gradual

**Space:** localised versus widely distributed

Their interaction produces four quadrants. With the same five drivers to each, we can construct four very different eventualities:




***1. "Chokepoint Shock":*** Armed groups with advanced C2 and kit strike at narrow but vital nodes—straits, pipelines, satellites. High-end capabilities diffuse to non-state actors via state patrons, global markets or rogue military elements trained in multi-domain operations. Local effects quickly scale because they touch global trade and critical infrastructure, carrying outsized consequences for international stability.

*Implication*: MDO's synchronised overmatch can clear or reopen such sites quickly, but adversaries define victory differently: simply enduring, being seen to resist, or inserting themselves into governance may serve their purpose as much as holding ground.

***2. "Preset Cascade"***: Dormant malware, long-range sea drones and other pre-programmed systems activate simultaneously across countries and domains when thresholds are met—a symbolic date, an environmental trigger. Cheap autonomy and ubiquitous coding let dispersed groups generate effects far beyond their size. Because the actions are automated, NATO's reaction cannot slow or stop them. The aims are nihilistic, designed less to achieve objectives than to unleash cascading disruption.

*Implication*: The adversary is automated and distributed; MDO's centralised synchronisation may be outpaced. Attribution and escalation management matter more than rapid firepower.

***3. "Attrition by Friction":*** Climate stress degrades NATO capabilities: energy-hungry data systems, aircraft, armour, sonar and satellites falter in hostile environments, while logistics chains are strained by heat and water scarcity. Small groups exploit these seams with modest attacks, knowing that operations are already under pressure. They also tap into new sources of legitimacy, presenting themselves as defenders of humanitarian relief or champions of environmental self-sufficiency.

*Implication*: Success depends less on shock and more on resilience, redundancy, and civil-military cooperation. Countering these threats requires building robustness into systems rather than preparing for a single decisive clash.

***4. "Bricolage Swarm"***: Terrorist tactics spread as know-how circulates through open channels—online guides, commercial tools, leaked military techniques. Small, scattered groups copy, adapt and remix methods across borders. These do-it-yourself networks may bring together actors with very different, even contradictory, aims, united only by a destructive or nihilistic impulse. The result is a dispersed pattern of violence that looks irregular and uncoordinated yet steadily erodes confidence and resources over time.

*Implication*: MDO struggles to find a decisive target. What matters is hardening societies and networks, as well as undermining the legitimacy that such bricolage actors draw from narrative and identity, rather than trying to out-gun adversaries.

**What Does This Exercise Tell Us?**

MDO is designed to overmatch adversaries by synchronising capabilities across domains. It assumes that threats can be anticipated and mapped, and that hierarchical adversaries can be broken by superior firepower and coordination. Where MDO is prepared for these assumptions to fail, as in Disaggregated Collaborative Air Operations, it is treated as the exception rather than the rule.

This makes MDO best suited to only one of the scenarios explored here: the *quick and small* case. In chokepoints or weak-governance zones where armed groups use advanced capabilities, NATO can concentrate force to reopen access or reassert control. This is also the scenario already visible today, from maritime harassment to strikes on infrastructure, and it is likely to grow in importance.

Even so, the exercise shows limits. MDO may succeed tactically in degrading an adversary but not in delivering strategic effect. Non-state actors operate to a different theory of victory, deriving legitimacy from resistance or survival rather than holding ground. And in strategically sensitive zones, NATO may also face constraints from rival patrons or covert great-power support.

**Beyond the "Quick and Small" Quadrant**

Looking across all four quadrants, a set of mismatches emerges between the logic of MDO, and the kinds of terrorist episodes NATO is likely to face. They do not all appear in every case, but many recur in three of the four scenarios, underlining how persistent the gaps are:

- **Centralised hierarchy vs decentralised networks.** NATO thrives on hierarchical planning and synchronised execution, while terrorist groups often disperse authority, relying on loose, adaptive networks that absorb disruption and regenerate quickly.
- **C2 vs zeal and initiative.** MDO assumes adversaries can be deterred or paralysed by loss of control. Terrorist actors, however, may be driven by ideological zeal or operate as self-directed lone actors, bypassing traditional C2 altogether and making disruption of leadership less decisive.
- **Integrated domains vs asymmetric ubiquity.** NATO links capabilities across domains to generate decisive advantage, but small groups frustrate this with cheap, resilient, low-tech methods.
- **Military dominance vs local legitimacy.** Firepower can reopen access or destroy targets, but rarely dislodges the legitimacy drawn from local ties and community presence.
- **Rapid innovation vs adaptive persistence.** NATO invests in cutting-edge systems; adversaries adapt incrementally to negate them and sustain pressure.
- **Duty vs sacrifice.** MDO values professional discipline and force protection, whereas terrorist groups may treat losses—or even martyrdom—as strategic assets.
- **Planned operations vs surprise.** NATO rehearses and sequences operations; terrorist actors often gain strength from improvisation and shock.
- **Territorial domains vs belonging and identity.** NATO maps conflict geographically, while groups define struggle by community, homeland or shared identity.
- **Threshold management vs ambiguity.** Terrorist incidents often fall below the level of war but above policing capacity, blurring attribution, escalation and legal authority.
- **Decisive timelines vs patient endurance.** MDO is geared to deliver swift, decisive effects across shifting great-power constellations. Terrorist groups are often single-issue and opportunist, measuring success in persistence over years or decades.

These recurring mismatches point to deeper asymmetries—of time, space, capability, legitimacy and cohesion—where MDO is systematically disadvantaged in CT.

**A Structural Challenge for NATO**

The deeper problem is organisational. When consensus is fragile, large bodies often ask the world to fit their doctrine rather than tailoring doctrine to the world. In CT this means rehearsing scenarios that validate MDO, rather than those that truly stress it. The Alliance's greatest strength—unity—can also become more than mere rhetoric, serving to signal coherence for deterrence while effectively sidelining the practical cooperation that CT demands.

MDO was not adopted through an open mapping of future eventualities, but as a means of preserving cohesion. As a US-inspired doctrine, it bound in a United States focused on peer rivalry with China. With its emphasis on joint service coordination, it also offered Europeans a way to manage burden-sharing and hold together states of different sizes and capabilities within multinational forces. The renewed focus on Russia in the East reinforced this approach and gave the appearance of a shared threat perception.

It is not hard to see how a terrorist attack could expose the limits of MDO—its reliance on pre-coordinated, multi-service, multinational effects—and risk cascading disruption across NATO itself.

**Conclusion: where MDO is at an asymmetric disadvantage**

By 2030, MDO will be expected to play a prime role in CT. But, in many plausible futures the doctrine does not map onto the adversary NATO is likely to face. The obvious corrective—adapting a doctrine built for marginal advantage in symmetrical conflict to asymmetric warfare—can and should go further. Terrorist groups, though weaker in conventional terms, enjoy asymmetric advantages in certain fields where MDO's assumptions about time, space, capability, legitimacy and cohesion do not hold.

- **Time as asymmetry.** NATO designed MDO for decisive outcomes in compressed timelines. Terrorist groups, by contrast, can afford to wait: single-issue, loosely connected, and opportunistic, they measure success in persistence over years or decades. Countering them requires CT mechanisms that endure beyond rotations, news cycles and intra-Alliance bargaining.
- **Space as asymmetry.** MDO defines geography through domains and extended theatres. Terrorist groups embed themselves in fragile states, urban margins and transnational networks where place and belonging matter more than maps. CT planning needs to integrate these "small geographies" alongside domain-based operations.
- **Capability as asymmetry.** MDO treats asymmetry as hardware gaps to be closed with superior platforms that bring mastery of terrain and domain. CT adversaries instead exploit environmental stress, redundancy gaps and low-cost tools. This makes

resilience—through hardened communications, redundant logistics and civil–military cooperation—more decisive than innovation and scale.

- **Legitimacy as asymmetry.** MDO equates success with battlefield dominance, especially shock and awe. Terrorist groups measure success in survival, visibility or narrative credibility. Battlefield defeat can even fuel legitimacy if framed as victimhood. This cannot be countered by firepower alone: CT must integrate information, governance and legitimacy-building measures.
- **Cohesion as asymmetry.** MDO was adopted in part to preserve Alliance unity—tying Europeans to a US doctrine shaped by rivalry with China and reaffirmed by the Russian threat. Terrorist groups, however, thrive on disunity, exploiting political cracks, uneven threat perceptions and blurred legal authority. The very diplomatic rationale that led to MDO's adoption risks turning it into a target, where small operational shocks can expose far larger divisions in the Alliance.

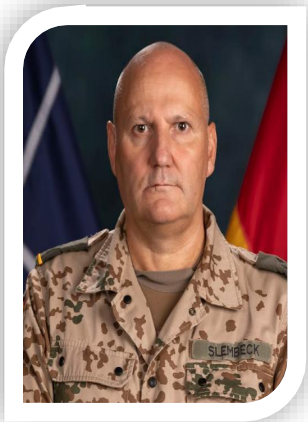
Recognising these asymmetries is the first step toward aligning MDO and CT in ways that stay effective through 2030 and beyond.

## *Session 2. NATO's Current CT Approach*

- ***Key Insight:*** *NATO remains reactive, relying on national requests rather than anticipatory strategies.*
- ***Policy Takeaway:*** *Permanent CT structures are needed at NATO level.*
- ***Operational Implication:*** *Current CT measures risk fragmentation without institutional anchoring.*
- ***Future Priority:*** *Institutionalize a NATO Counter-Terrorism Directorate within HQ.*

# NATO's Current Prospective on Counter-terrorism

*LTC Claus SLEMBECK – SME at HQ ACT NATO*




**Introduction**

The security environment of the twenty-first century is marked by an evolving blend of conventional and unconventional threats. While NATO remains focused on great-power competition and traditional defence obligations, terrorism continues to represent one of the most complex and persistent challenges to international stability. Terrorist groups adapt rapidly to technological innovation, environmental pressures, and shifting geopolitical landscapes, exploiting vulnerabilities in states and societies. This evolving threat environment requires NATO to reassess its counter-terrorism posture and refine its strategic approach.

This paper outlines NATO's current perspective on counter-terrorism, presenting the central challenges posed by transnational terrorism, the likely characteristics of terrorist threats in the coming decades, and the avenues through which NATO can enhance its response. It underscores the importance of aligning military and non-military instruments, coordinating with national and international civilian authorities, and strengthening the resilience of societies.

**Transnational Networks and the Limits of Unilateral Action**

The fight against terrorism is inherently international. Transnational terrorist and illicit networks function across borders, often with a sophistication that allows them to bypass traditional state-based controls. These networks operate fluidly between domains, exploiting gaps in governance and regulation. No single government or organization possesses the capacity to dismantle them in isolation. Instead, effective counter-action requires synchronized and net-centric responses at global, regional, and sub-regional levels.

For NATO, this recognition creates both opportunities and constraints. While the Alliance has unparalleled capacity in terms of military coordination, deterrence, and strategic communication, many of the core functions necessary to counter terrorism—such as law enforcement, financial monitoring, and intelligence collection—remain the prerogative of nation states and specialized civilian organizations. NATO therefore faces a structural dilemma: it is well positioned to support and integrate counter-terrorism efforts but less suited to orchestrate them in a comprehensive sense. Without a framework that bridges these institutional seams, the international community risks leaving critical gaps in its collective ability to disrupt transnational threats.

**Anticipating the Future of Terrorism**

Looking ahead over the next 15 to 20 years, terrorism is expected to evolve along several trajectories shaped by technology, climate change, decentralized organization, and geopolitics. Although uncertainty will always cloud predictions, current trends allow for plausible scenarios.

Technological advances will almost certainly play a central role. Terrorist actors may adopt artificial intelligence to enhance their operational capabilities, deploying autonomous drone swarms, developing methods to evade recognition systems, or using deepfake technology to manipulate public perception. Cyberterrorism is also likely to intensify, as smart cities and increasingly digitized infrastructure provide vulnerable targets. The objective of such attacks may not be high casualty rates but the deliberate creation of chaos and paralysis. Advances in synthetic biology add another layer of risk, raising the possibility of engineered viruses or bacteria being used as weapons.

In parallel, climate change will drive new sources of instability that terrorist groups may exploit. As environmental stress deepens through droughts, food scarcity, and population displacement, ideologically motivated eco-terrorism could emerge. Groups might target natural resources such as water and agriculture, either in pursuit of environmental causes or as a deliberate strategy to destabilize governments.

Another defining feature of future terrorism will be its organizational form. Increasingly decentralized and networked groups are expected to replace traditional hierarchical structures. Inspired by online propaganda, individuals or small cells may act independently, complicating detection and prevention. Financing may also evolve through blockchain and other decentralized platforms, making the tracking of money flows more difficult for authorities.

Finally, shifting geopolitical dynamics will create fertile ground for new forms of extremism. Power vacuums in fragile states, exacerbated by corruption, conflict, or climate stress, will provide safe havens for terrorist groups. Ideological motivations may diversify beyond religious extremism to include anti-artificial intelligence radicalism, neo-Luddism, and extreme nationalism. This diversification will demand flexible responses and the avoidance of overly narrow threat perceptions.

**NATO's Strategic Approach**

In response to this evolving landscape, NATO identifies several areas where it can build comparative advantage. The Alliance's capacity does not rest solely in its military power but also in its ability to foster multinational cooperation, promote resilience, and integrate technological innovation into its counter-terrorism strategies.

From a cognitive standpoint, NATO can strengthen its role in countering terrorist narratives. This includes developing databases to identify vulnerable audiences, embedding liaison nodes within law enforcement and international agencies, and building the capacity of allies and partners to combat disinformation and propaganda. By shaping coherent narratives

and exposing state support for terrorist actors, NATO can contribute to delegitimizing extremist ideologies.

In the cyber domain, NATO must be prepared to adopt offensive as well as defensive measures. Partnering with private technology companies and broadening cooperation into a digital alliance will be critical. Intelligence fusion—integrating human, signals, and surveillance intelligence—will provide a more comprehensive understanding of the threat environment.

Resilience is another essential dimension. NATO can work with Allies to identify vulnerabilities in critical infrastructure and societal systems, reinforcing preparedness against terrorist disruptions. Partnerships with industrial sectors can accelerate the integration of new technologies into counter-terrorism operations, particularly in areas such as counter-unmanned aerial systems and emerging disruptive technologies.

Geographically, NATO must adapt its partnerships to the regions, most vulnerable to terrorism. The Sahel, where weak governance intersects with conflict and external influence, requires particular attention. NATO has the potential to degrade both terrorist and destabilizing state activities in the region while synchronizing efforts with international organizations. The aftermath of the Russia-Ukraine war also presents risks of weapons proliferation and illicit technology transfer, making coordinated action even more urgent.

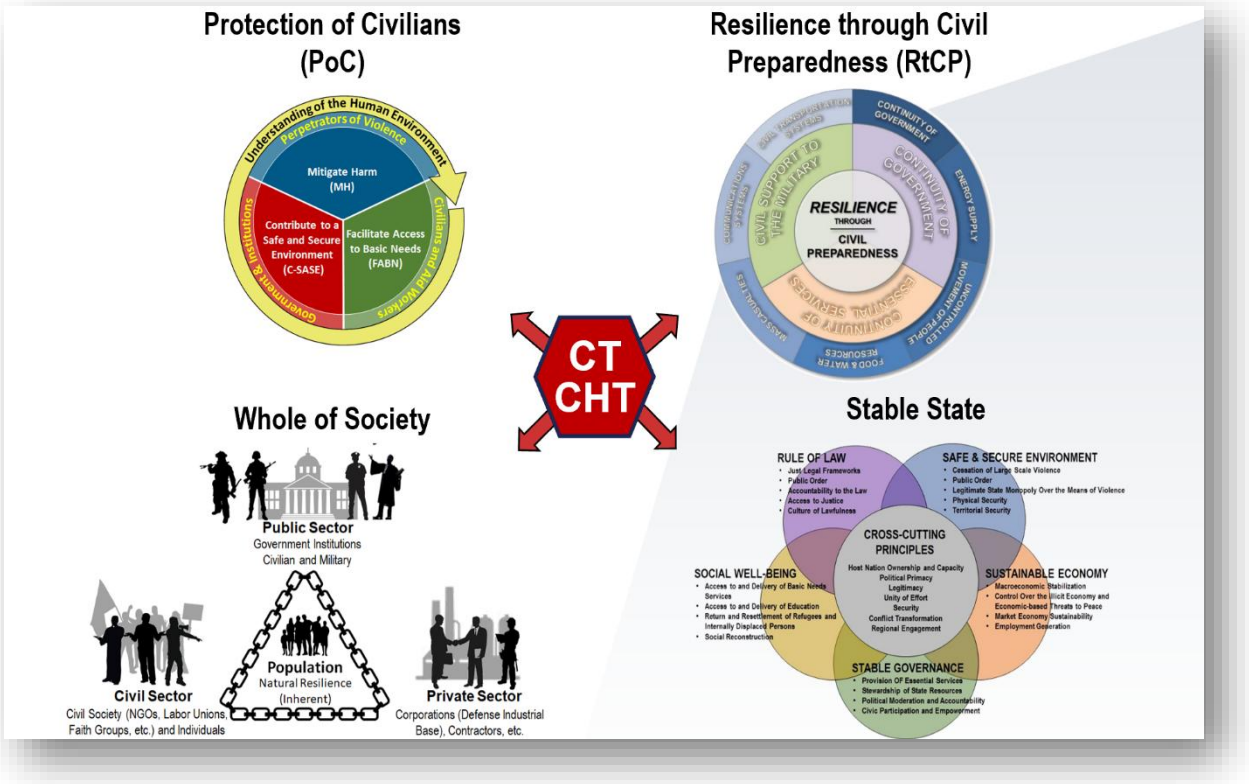



*Figure 4 CHT/CT - Useful Models Informing Policy and Strategy Development*

## Policy and Strategic Implications

The implications for NATO policy are significant. The current counter-terrorism policy framework is outdated and does not reflect the realities of emerging threats. A revised framework must be forward-looking, realistic, and adaptable to future developments. It must situate terrorism within the broader context of unrestricted warfare, where the boundaries between conventional conflict, terrorism, and hybrid threats are increasingly blurred.

Conceptual models can help inform this evolution. The protection of civilians must remain a cornerstone of NATO's legitimacy, while resilience through civil preparedness ensures societies are able to withstand shocks. A whole-of-society approach acknowledges the indispensable contributions of civilian actors, private industry, and communities. Finally, the stable state model highlights the importance of addressing fragility and governance gaps that terrorists routinely exploit.

## Core Objectives for NATO

To remain effective, NATO must pursue four interlinked objectives. The first is to enhance security coordination by encouraging more efficient intelligence exchange among states and NATO structures. The second is to strengthen societal resilience, reducing polarization and social tensions that create openings for radicalization. The third is to advance technological defence, ensuring that Allies' digital infrastructure is safeguarded against cyberterrorism and related threats. Finally, NATO must contribute to tackling disinformation by promoting transparency and trust, which are essential in preventing extremist narratives from taking root.

## Conclusion

Terrorism will remain a defining challenge for NATO in the decades to come. Its transnational, adaptive, and multifaceted nature requires a response that is equally dynamic and comprehensive. NATO is not the sole actor responsible for counter-terrorism, yet it holds a pivotal role in facilitating coordination among Allies, reinforcing societal resilience, and leveraging both military and non-military tools.

The path forward lies in developing a counter-terrorism strategy that integrates cognitive, cyber, resilience, and geographical advantages while aligning with civilian frameworks at the national and international levels. By strengthening coordination, embracing technological innovation, and supporting resilient societies, NATO can ensure that terrorism does not undermine global security and stability.

# The Future of NATO and Counter-terrorism

*Assoc. Prof. Özgür KÖRPE – Turkish National Defence University*

**Introduction**

This paper traces the evolution of NATO's counter-terrorism (CT) posture from the post-Cold War era to the present, and projects its possible trajectories toward 2030. It argues that terrorism has consistently been recognized as a persistent asymmetric threat within NATO's security agenda, especially since the 9/11 attacks. Over time, NATO has transitioned from a tactical crisis-response mindset to a broader strategic adaptation, integrating counter-terrorism into long-term foresight, technological innovation, and multi-domain operational planning.

**Strategic Foresight and Analytical Foundations**

The 2023 Strategic Foresight Analysis (SFA23) is presented as a cornerstone document. Extending NATO's horizon to 2043, it frames terrorism and violent non-state actors as enduring drivers of instability. SFA23 emphasizes foresight and resilience, urging the Alliance to embed CT considerations into force development, capability planning, and decision-making. The analysis highlights not only the threat itself but also the systemic environment—climate instability, fragile governance, technology diffusion—that shapes terrorism. NATO's challenge, therefore, is not simply to respond but to anticipate, adapt, and integrate CT into its broader deterrence posture.

**Policy Guidelines and Technological Emphasis**

Building on this foresight, the 2024 Revised Counter-Terrorism Policy Guidelines refine NATO's 360-degree approach around three functional pillars: prevention, protection, and response. The Guidelines explicitly foreground emerging and disruptive technologies (EDTs) such as artificial intelligence, autonomy, and quantum-secure communications. They also stress whole-of-Alliance resilience, information sharing, and preparedness for chemical, biological, radiological, and nuclear (CBRN) attacks. NATO's counter-terrorism vision is thus not narrowly military but integrated across civil-military domains, societal preparedness, and technological innovation.

These Guidelines are operationalized through NATO exercises—live, command-post, and tabletop—testing asymmetric responses, hybrid threat resilience, and legal frameworks. They are also disseminated via capacity-building programs with partners such as Georgia, Jordan, and Iraq, where modular curricula and institutional mentoring align national practices with NATO standards.

**Hague Summit 2025: Institutionalizing Counter-Terrorism**

The Hague Summit of June 2025 reinforced the Guidelines' trajectory. Five decisions stand out. First, terrorism was reaffirmed as a persistent threat alongside state-based adversaries, embedding CT firmly within NATO's three core tasks: deterrence and defence, crisis management, and cooperative security. Second, allies committed to increasing defence spending, projecting 5% of GDP by 2035, to sustain CT-related research, capability regeneration, and resilience programs. Third, the Summit addressed the need to strengthen the transatlantic defence industrial base, particularly in producing munitions, sensors, and technologies relevant to CT. Fourth, NATO sought to accelerate decision-making cycles, introducing pre-delegated authorities to support rapid response. Fifth, EU–NATO cooperation was deepened in border security, maritime interdiction, and cyber incident response. Collectively, these measures aimed to ensure CT was not marginal but mainstreamed into NATO's deterrence and defence posture.

**Four Analytical Pillars for Future CT**

The paper then develops a forward-looking roadmap structured around four analytical domains—Awareness, Capabilities, Engagement, and Cooperation—which complement NATO's official prevention, protection, and response framework. Each domain is mapped into near-, mid, and long-term initiatives.

**Awareness**

The priority here is improving intelligence sharing, foresight, and situational awareness. Near-term proposals include an AI-augmented Intelligence Liaison Unit at ACO Mons, expansion of the Southern Hub's data feeds, and privacy-enhancing data-sharing frameworks. By the mid-term, NATO could field a federated intelligence mesh and integrate AI-driven intent prediction models, while incorporating gender and human-security perspectives into threat assessments. By 2029–2030, predictive awareness platforms would continuously forecast terrorist safe havens, linked to civilian resilience indicators.

**Capabilities**

This pillar emphasizes operational preparedness, anchored in NATO's Defence Against Terrorism Programme of Work (DAT POW). Near-term actions involve upgrading field kits with advanced CBRN detectors, standardizing training via AI-assisted simulations, integrating Turkish military education reforms (scenario-based MDMP labs, multi-domain operations training, digital staff rides), and acquiring counter-UAS modules. Mid-term measures include deploying autonomous perimeter-defence swarms, adopting quantum-resistant cryptography, and harmonizing doctrine with national special operations forces. Long-term ambitions include globally deployable modular CT packages and predictive maintenance of CT platforms using digital twins and AI prognostics.

Türkiye's recent military education reform conducted within the Turkish National Defence University—centred on scenario-based MDMP laboratories, MDO training modules,

digital staff rides, and a modernized professional military education (PME) curriculum within the Turkish National Defence University—stands out within this capability domain. These reforms accelerate the alignment of national training institutions with NATO's evolving CT and MDO doctrines while generating transferable "best practice" models for allied professional military education. As a result, Türkiye is not only a force contributor but also an institutional learning hub whose innovations help shape NATO's long-term capacity-development trajectory. This contribution illustrates how national reforms can reinforce the Alliance's collective CT ecosystem and operational readiness.

**Engagement**

Engagement is linked to the response pillar, centring on strategic communication, civil-military coordination, and counter-narratives. In the near-term, NATO is urged to expand the Strategic Communications COE's data-science cells, embed CT modules into Partnership for Peace curricula, and prototype adaptive counter-narrative platforms. By 2027–2028, engagement would scale to AI-driven audience segmentation, a permanent CT engagement forum with civil society and tech actors, and the development of a CT Engagement Index. By 2030, NATO would transition to a cloud-native, multilingual communications ecosystem and deploy AI mediators in online forums to pre-empt radicalization threads.

**Cooperation**

The cooperation pillar stresses institutional partnerships. Near-term ideas include launching an EU–NATO CT Hybrid Fusion Cell, harmonizing data-sharing agreements, and convening annual NATO–UN workshops on CBRN and evacuation readiness. Mid-term proposals envision a NATO-led public-private R&D consortium, interoperable training accreditations, and liaison officers to regional CT hubs. By 2029–2030, NATO could operationalize a "one-stop CT ecosystem" portal integrating EU, UN, and INTERPOL resources, alongside a rotating CT innovation fellowship program.

**Multi-Domain Counter-Terrorism**

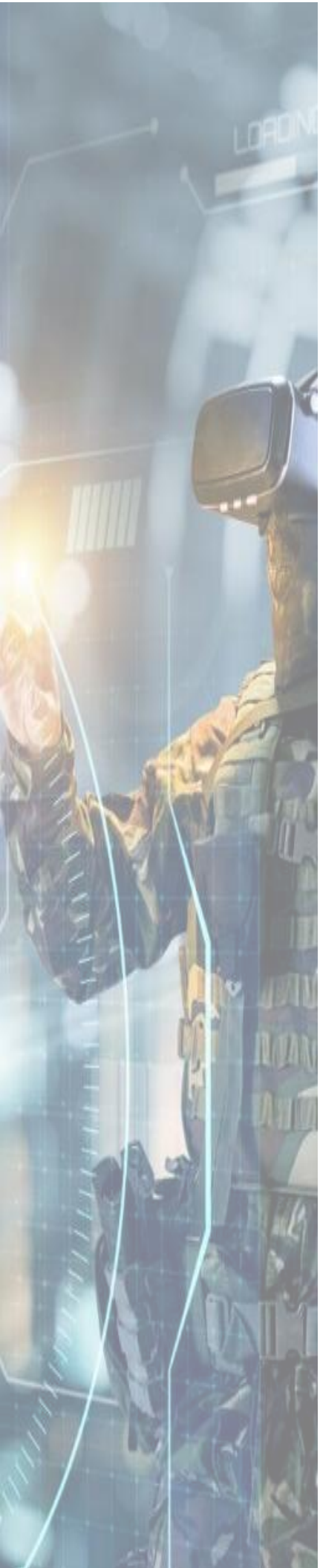
The paper underlines the need to embed CT into NATO's MDO Concept. Three offers are proposed. First, establish a NATO MD-CT Integration Hub that co-locates analysts, operators, and technologists, while publishing a CT Multi-Domain Concept Addendum. Second, deploy modular CT rapid response forces validated through multi-domain exercises, with tailored packages across land, air, maritime, cyber, space, and information domains. Third, institutionalize MD-CT training, legal alignment, and fellowship exchanges with EU, UN, and civil society partners, ensuring both doctrinal innovation and legal interoperability.

**Concluding Reflections**

The conclusion identifies three imperatives. First, technological convergence: the proliferation of autonomous drones, AI systems, and cyber-physical attacks requires accelerated joint R&D and interoperable defences. Second, evolving threat vectors: climate-induced

instability, hybrid tactics, and diffusion of WMD materials compel NATO to expand beyond kinetic CT to include resilience planning and recovery frameworks. Third, strategic agility: NATO must refine legal and policy frameworks to enable rapid deployment and secure data sharing.

Ultimately, the article portrays NATO's CT strategy as an evolving blend of foresight, technology, and cooperation. The Alliance must continuously balance doctrinal convergence with the contextual realities of member states, acknowledging that while shared frameworks are possible, operational replication may remain uneven. Türkiye's contributions in military education reform are highlighted as examples of how national innovations can feed into NATO's collective CT ecosystem.



## *Session 3. CT and Future Warfare Trends*

- ***Key Insight:*** *Emerging technologies are low-cost for terrorists but high-cost for NATO to counter.*
- ***Policy Takeaway:*** *Counter-terrorism must anticipate rapid innovation cycles, especially in drones and AI.*
- ***Operational Implication:*** *Training must include OSINT and red-teaming exercises on AI-enabled threats.*
- ***Future Priority:*** *Establish rapid adaptation protocols for tech-driven terrorist tactics.*

# Contemporary CT Approaches from a Critical Perspective

*Prof. Michael LISTER – Oxford Brookes University*

## Introduction

This paper introduces the key ideas of Critical Terrorism Studies (CTS) and applies them to the debates around Multi-Domain Operations (MDO), especially regarding the integration of civil society and citizens into counter-terrorism governance. While recognizing potential benefits in involving non-state actors, the analysis highlights significant risks and unintended consequences. The central concern is that efforts to extend counter-terrorism beyond state institutions may generate discriminatory practices, undermine public trust, and complicate coordination.

## Critical Terrorism Studies: Challenging the Mainstream

CTS emerged in the mid-2000s as a reaction to what scholars termed "orthodox" terrorism studies. Writers such as Richard Jackson, Jeroen Gunning, and others criticized the dominant approach for four reasons: it treated terrorism as an objective phenomenon rather than a socially constructed label; it focused almost exclusively on non-state actors while neglecting state violence; it relied heavily on secondary sources rather than primary data; and it concentrated disproportionately on the global North.

CTS therefore redirected attention toward language, discourse, and power. A major theme is the inconsistent application of the "terrorism" label. Historical and contemporary examples—from Nelson Mandela's long listing on the U.S. terror watchlist to current debates in the UK about whether certain violent acts (e.g., the Southport attack or Palestinian Action protests) should be deemed terrorism—illustrate the contested and political nature of designation. Jackson argues that terrorism is not a "brute fact" but a "social fact": acts of violence are concrete, but their classification depends on interpretation, context, and political framing.[1]

CTS also studies the consequences of this labelling. Once violence is called "terrorism," governments and societies often authorize extraordinary measures. Barack Obama's 2015 observation that the U.S. spends over a trillion dollars on counter-terrorism while failing to legislate against gun deaths exemplifies the disproportionate responses that terrorism discourse

[1] Richard Jackson, *Writing the War on Terrorism: Language, Politics and Counter-terrorism* (Manchester: Manchester University Press, 2005); Richard Jackson, "Constructing Enemies: 'Islamic Terrorism' in Political and Academic Discourse," *Government and Opposition* 42, no. 3 (2007): 394–426.

generates. Thus, CTS critiques both the definitional inconsistency and the discursive power that enables exceptional security practices.

**Shifting the Focus to Citizens and Civil Society**

Applying CTS insights to MDO highlights how counter-terrorism governance has expanded beyond the state. Scholars such as Jarvis and Lister have documented how research increasingly explores not only what governments do but also how citizens and private actors are enrolled into security provision. Lister's own studies emphasize how private companies are now legally tasked with counter-terrorism duties.[2]

In the UK, this trend is most visible in legislation. The Counter-Terrorism and Security Act 2015 introduced the Prevent Duty, legally obligating teachers, doctors, and other public sector workers to identify signs of radicalization. More recently, the Terrorism (Protection of Premises) Act 2025 requires public and private venues—from restaurants to sports stadiums—to maintain counter-terrorism plans and training. These measures represent what Krzysztof Feliks Sliwinski calls the "civilianisation" of counter-terrorism.[3]

This development parallels the rationale of MDO: integrating diverse domains and institutions, enabling information-sharing, and orchestrating coordinated activities across military and non-military actors. German defence policy explicitly notes that MDO effectiveness increases when combined with non-military actions. Civil society, although not formally a military domain, is thus pulled into a wider whole-of-government approach.

**Co-Production and the Logic of Civilianisation**

The incorporation of non-state actors reflects broader public policy trends of "co-production," where governments enlist citizens and institutions in service delivery. While this aligns counter-terrorism with wider governance practices, it also raises challenges familiar from other domains: issues of legitimacy, capacity, and unintended effects.

In counter-terrorism specifically, three areas of concern stand out: discrimination and prejudice, paradoxical insecurity, and coordination difficulties.

**Risk One: Discrimination and Prejudice**

A major danger of mobilizing civil society in counter-terrorism is the reinforcement of racism, Islamophobia, and other exclusionary practices. When ordinary citizens, teachers, or private employees are encouraged to monitor "suspicious behaviour," the judgments they make

---

[2] Michael Lister, "Security Professionals and Public Opinion: Legitimacy, Publicity and Brand Identity," *Politics*, published ahead of print, January 2025; Michael Lister, *Public Opinion and Counter-Terrorism: Security and Politics in the UK* (London: Routledge, 2023).

[3] Krzysztof F. Sliwinski, "Counter-terrorism – a Comprehensive Approach: Social Mobilisation and 'Civilianisation' of Security: The Case of the United Kingdom," *European Security* 22, no. 3 (2012): 288–306.

often reflect dominant stereotypes about minority groups. Some scholars argue that the "vigilant gaze" promoted by public-facing counter-terrorism campaigns reproduces racial hierarchies, while others warn that marginalized populations, including autistic and neurodivergent individuals, risk being misclassified as threatening because they do not fit social norms.

Empirical evidence supports these critiques. In the UK, the Prevent strategy has been widely criticized for Islamophobic profiling and for flooding authorities with poor-quality referrals. Comparable patterns have been documented in some other examples, where community policing and counter-terrorism measures display exclusionary dynamics. Such practices waste resources, undermine intelligence quality, and erode social cohesion.

**Risk Two: Security Versus Insecurity**

A second paradox is that measures designed to enhance security may produce greater feelings of insecurity. Research has shown that visible fortifications and protective measures in urban spaces can create unease among inhabitants. By constantly drawing attention to potential risks, governments may cultivate what some scholars describe as the "neurotic citizen"—someone perpetually anxious about terrorism.

Further studies demonstrate how efforts to transform citizens into "counter-terrorism actors" intensify fear and normalize the securitisation of everyday life. Rather than empowering communities, this process can amplify the psychological impact of terrorism itself. Moreover, by inviting citizens to demand greater policing and surveillance, these dynamics risk encouraging authoritarian impulses. Well-intentioned inclusionary policies can, in practice, expand state control and even promote forms of vigilantism.

**Risk Three: Coordination and Command Challenges**

The third major problem lies in coordination. Research on multi-domain operations acknowledges the difficulty of synchronizing multiple domains. The inclusion of civil society further compounds this complexity. Some private security companies are well aligned with counter-terrorism frameworks and profit from security provision. In contrast, other businesses—such as social media platforms or real estate developers—may resist or only partially comply because counter-terrorism responsibilities conflict with their core commercial models. These have been described as "reluctant security actors," since commercial incentives often run counter to security requirements.

This unevenness raises questions about reliability, accountability, and integration. Involving actors with divergent motivations risks fragmenting rather than strengthening governance in the field of counter-terrorism.

**Implications for Multi-Domain Operations**

The broader implication for MDO is that incorporating civil society is not automatically positive. While it may extend capacity and distribute responsibility, it can also entrench discriminatory practices, generate fear, and complicate coordination. For NATO and other alliances considering how to adapt MDO concepts to counter-terrorism, these lessons are critical. They suggest that the enthusiasm for "whole-of-society" approaches must be tempered by awareness of their risks.

In practice, integrating non-military actors into MDO requires safeguards: strong anti-discrimination frameworks, careful attention to psychological impacts on citizens, and mechanisms to reconcile divergent institutional logics. Without these, civilianisation could weaken rather than strengthen counter-terrorism.

**Conclusion**

This paper situates CTS within contemporary debates on counter-terrorism and MDO. CTS critiques the mainstream for essentializing terrorism and neglecting the politics of labelling. It shifts attention to discourse, power, and the societal consequences of security practices. When applied to MDO, CTS highlights the risks of extending counter-terrorism into civil society.

Three dangers are particularly salient. First, reliance on citizens and private actors can reproduce racial and social prejudice, leading to misidentification of threats and flawed intelligence. Second, attempts to mobilize civilians as counter-terrorism actors may ironically foster insecurity and fear, producing "neurotic citizens" and strengthening authoritarian demands. Third, coordination between diverse actors with conflicting logics—ranging from private security firms to reluctant corporate participants—poses significant operational challenges.

The lesson for MDO is caution: while civilian participation may appear to expand capacity, it also carries unintended consequences. Critical perspectives encourage policymakers to reflect not only on efficiency and integration but also on justice, legitimacy, and the lived experience of security. Counter-terrorism that alienates minorities, heightens public anxiety, or undermines democratic norms risks eroding the very resilience it seeks to build.

# Future Warfare and the Future of Terrorism: Means and Instruments

*Dr. Ridvan Bari URCOSTA – NATO Defence College Fellow*

**Introduction**

The rapid pace of technological change and the increasing convergence of military and civilian domains are reshaping the character of warfare in the twenty-first century. Traditional distinctions between strategic and conventional forces, once sufficient to capture the scope of conflict, are being transformed by the emergence of new domains such as cyber, space, and unmanned systems. These are not simply additive layers to existing capabilities; they mark a transition toward what some theorists call "Singularity Warfare," a paradigm where artificial intelligence, robotics, quantum systems, and cognitive operations converge to create a qualitatively new battlespace.

This transformation has profound implications for terrorism. As state and non-state actors alike adapt to the new technological environment, terrorism is poised to become more asymmetric, more decentralized, and more integrated with advanced technologies. The following narrative explores how the future of terrorism may evolve within the broader framework of future warfare, with particular attention to the means and instruments that will shape this evolution.

**The Concept of Singularity Warfare**

After the Second World War, modern warfare was generally divided into two categories: strategic forces, including nuclear deterrence, and conventional forces spanning land, sea, and air. Over recent decades, however, three additional forces—cyber, space, and drone capabilities—have emerged as decisive factors. Together with advances in artificial intelligence and quantum physics, these developments are converging into what is increasingly described as Singularity Warfare.

This concept refers to the integration of all operational domains into a unified battlespace in which traditional rules no longer apply. Like a chess game where the board, the pieces, and even the rules change continuously, future warfare will be fluid, dynamic, and unpredictable. Artificial intelligence, large language models, robotics, and quantum systems will not merely supplement human decision-making but in many cases surpass it, accelerating the tempo of operations beyond human cognitive limits.

Chinese military doctrine has already identified this tipping point. As early as 2016, the Chinese Ministry of Defence argued that the accelerating integration of AI and human-machine

technologies would lead to a singularity in which human brains could no longer cope with the pace of battlefield dynamics. Decision-making, they predicted, would shift to intelligent machines, with human operators relegated to supervisory roles. This "human-on-the-loop" model signals a fundamental break with millennia of warfare premised on human command.

**Historical Antecedents and Intellectual Roots**

Although Singularity Warfare is a modern term, the intellectual roots of the idea extend back decades. John von Neumann in 1958 observed that accelerating technological progress gave the appearance of humanity approaching a "singularity" beyond which traditional patterns of life could not continue.[1] Vernor Vinge in 1983 predicted the creation of intelligence surpassing human capacity, initiating an unstoppable transformation toward a "post-human" era.[2] More recently, voices from the technology sector, such as Sam Altman, have argued that humanity has already passed the event horizon of digital superintelligence.[3]

These perspectives underscore a critical reality: once the singularity threshold is crossed, the pace of change accelerates in ways that are difficult for governments and institutions to control. Every scientific revolution in history has transformed social and political systems, and the singularity promises to be no different. The rise of machine intelligence and autonomous systems will inevitably provoke not only new forms of warfare but also social resistance, ideological backlash, and potentially even terrorism rooted in opposition to technological dehumanization.

**Neo-Luddism and the Future of Terrorist Motivations**

Historical parallels can be drawn with the Luddite movement of the nineteenth century, when workers destroyed machinery in protest against industrialization and technological unemployment. In the modern era, similar anxieties are resurfacing in what is termed "neo-Luddism." Manifestos such as Ted Kaczynski's *Industrial Society and Its Future* expressed the fear that technology erodes human freedom and degrades the environment. Such anti-technological ideologies may become increasingly influential as artificial intelligence, automation, and biotechnology reshape human societies.

Future terrorism may thus be motivated not only by religious or political ideologies but also by opposition to technological change itself. Groups may emerge that reject machine intelligence, resist digital integration, or exploit public fears about dehumanization. This

---

[1] Stanislaw Ulam, "Tribute to John von Neumann," *Bulletin of the American Mathematical Society* 64, no. 3 (1958): 1–49.

[2] Vernor Vinge, "The Coming Technological Singularity: How to Survive in the Post-Human Era," *Vision-21: Interdisciplinary Science and Engineering in the Era of Cyberspace*, NASA Conference Publication 10129 (1993): 11–22.

[3] Sam Altman, "Planning for AGI and Beyond," *OpenAI Blog*, February 24, 2023, https://openai.com/blog/planning-for-agi-and-beyond.

expansion of terrorist motivations underscores the unpredictability of the threat landscape in the era of Singularity Warfare.

**Terrorism and Artificial Intelligence**

Perhaps the most consequential development is the symbiosis between artificial intelligence and terrorism. AI has the potential to act as a "force multiplier" for terrorist groups, enabling them to act with the sophistication of a grandmaster against amateur opponents. Large language models, chatbots, and machine-learning systems are already being exploited by extremist groups. Reports indicate that ISIS operatives began using ChatGPT as early as 2022 to support logistical planning, propaganda dissemination, and recruitment.

AI can provide terrorists with detailed instructions for constructing weapons, planning missions, or evading surveillance. It can simplify operational schedules, generate persuasive narratives, and tailor recruitment messaging to specific audiences. As algorithms become more human-like, they also risk creating addictive feedback loops, particularly for disaffected individuals who may bond with AI companions. Counter-terrorism practitioners have begun experimenting with AI-driven chatbots trained on extremist worldviews, both to study radicalization processes and to develop tools for counter-radicalization.

The most troubling prospect is the potential emergence of AI agents acting as autonomous terrorists. While speculative, the notion of reflective or "thinking" weapons—systems that penetrate cognitive spaces and make independent decisions—raises unprecedented ethical and strategic questions.

**The Drone Revolution**

Unmanned aerial systems exemplify the asymmetric potential of modern technologies. Drones are relatively cheap, widely available, and increasingly capable of precision targeting. The war in Ukraine has demonstrated how small teams can build and deploy drones with significant effect, sometimes using improvised parts. These systems can strike deep into enemy territory, bypass traditional defences, and inflict strategic damage on critical infrastructure.

For terrorist groups, drones represent an ideal tool of asymmetric warfare. They can be produced clandestinely, deployed unpredictably, and adapted for diverse missions ranging from surveillance to direct attacks. Emerging tactics, such as the "Matreshka" model of layered autonomy—where a single unmanned system carries smaller autonomous systems for different tasks—illustrate how drones may evolve into multi-layered, multi-tasking platforms. The diffusion of such capabilities means that even non-state actors can now pose strategic threats once reserved for state militaries.

**Cognitive and Information Domains**

Beyond physical instruments, the future of terrorism will be shaped by control over the cognitive and informational domains. Terrorist groups have long exploited media to amplify their impact, but new technologies intensify this dynamic. Artificial intelligence can generate deepfakes, tailor propaganda to individual psychological profiles, and flood digital ecosystems with manipulative content.

Equally, intelligence agencies are already experimenting with penetrating societies through social networks and fake accounts, as evidenced in recent operations in the Middle East. Such techniques blur the line between terrorism, insurgency, and statecraft. In the future, the distinction between psychological and kinetic warfare may collapse entirely, with both converging in the singular battlespace.

**Strategic Implications**

The convergence of these technologies raises critical questions for states and alliances such as NATO. The traditional monopoly of the state over advanced military systems is eroding as non-state actors gain access to AI, drones, and decentralized production. Counter-terrorism strategies must therefore account for the diffusion of capabilities once thought unattainable for terrorist groups.

Defence against AI-driven terrorism will require not only technological countermeasures but also regulatory frameworks governing the use of machine learning systems, ethical standards for autonomy in weapons, and international cooperation on cybersecurity. Similarly, resilience against drone attacks will demand new forms of infrastructure protection, dispersion of assets, and counter-unmanned systems.

Most importantly, counter-terrorism must expand into the cognitive domain. Preventing radicalization in the age of AI will involve not only traditional education and community engagement but also the development of counter-algorithms capable of disrupting extremist narratives online. The future of counter-terrorism may hinge as much on the battle for minds and information flows as on the control of territory.

**Conclusion**

The future of warfare and terrorism is being shaped by the onset of Singularity Warfare, where the boundaries between human and machine, physical and digital, conventional and cognitive, are increasingly blurred. Terrorism will adapt to this new environment, exploiting artificial intelligence, drones, decentralized production, and information manipulation to offset the superior power of states. Motivations may expand to include not only religious or political extremism but also ideological opposition to technology itself.

For policymakers, the challenge is immense. The speed of technological change threatens to outpace the ability of institutions to adapt. Yet the stakes are clear: failure to anticipate the convergence of future warfare and terrorism risks leaving societies vulnerable to asymmetric attacks of unprecedented scale and sophistication. The imperative, therefore, is to invest in resilience, regulation, and innovation, ensuring that counter-terrorism remains effective in an age where the very logic of war is being rewritten.

## *Session 4. CT Integration into MDO*

- ***Key Insight:*** *CT is still treated as a "side dimension" of MDO, not a core pillar.*
- ***Policy Takeaway:*** *NATO doctrine must recognize terrorism as a multidomain adversary equal to peer threats.*
- ***Operational Implication:*** *Civilian, private, and military actors must be embedded in CT-MDO planning.*
- ***Future Priority:*** *Create joint NATO–civilian/private taskforces for CT within MDO exercises.*

# Counter-Terrorism in MDO Environment

*Assoc. Prof. Emrah ÖZDEMİR – Turkish Military Academy*

**Introduction: Understanding the Essence of MDO**

MDO represent a significant evolution beyond traditional joint operations. While joint operations coordinate actions across land, air, and maritime domains, MDO go further by integrating all five operational domains—land, air, maritime, cyber, and space—in a highly synchronized, simultaneous, and continuous manner. The aim is not only to coordinate but to create cross-domain synergy that enables overmatch, disrupts adversaries' decision-making processes, and achieves strategic objectives with speed and precision.

*"MDO is the orchestration of military activities across all domains [land, air, maritime, cyber, and space] and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance" (Allied Joint Publication AJP-0.1F).*

This explanation emphasizes the need for not only domain integration but also the fusion of military and non-military efforts to generate decisive effects in complex and contested environments.

Furthermore, MDO should be viewed as an essential element of a broader, whole-of-government and whole-of-alliance approach. It operates in concert with the Diplomatic, Informational, Military, and Economic (DIME) instruments of power, ensuring a comprehensive strategy to deter, compete with, and, if necessary, defeat adversaries.

In essence, MDO in the NATO framework is about delivering converging, synchronized, and adaptive effects across all domains and instruments of power, enabling the Alliance to respond decisively and effectively in an increasingly interconnected and contested strategic environment.

**Origins of MDO**

The concept of MDO emerged in response to the growing complexity of modern warfare, where threats transcend traditional boundaries and domains. Initially developed within the U.S. military, particularly by the U.S. Army, MDO has since evolved into a comprehensive operational and strategic framework that has been increasingly adopted by NATO.

In the 1980s, the U.S. Army introduced the AirLand Battle doctrine, integrating air and land operations to counter the Soviet threat. This was an early step toward cross-domain thinking.

After the Cold War, the focus shifted to joint operations, coordinating across land, air, and maritime forces. However, the emergence of near-peer adversaries and challenges like China and Russia—who developed Anti-Access/Area Denial (A2/AD) strategies—pushed military

planners to consider the full spectrum of conflict, including cyber, space, and the electromagnetic spectrum.

In 2018, the U.S. Army introduced its initial MDO concept to address these emerging threats, though it remained a conceptual effort at that time. This changed in October 2022, when the Army published the updated Field Manual (FM) 3-0, establishing MDO as its official doctrine for operations during competition, crisis, and conflict.

Over time, MDO expanded beyond a single-service approach to become a strategic-level framework, guiding how militaries integrate all domains and instruments of power to achieve decisive outcomes.

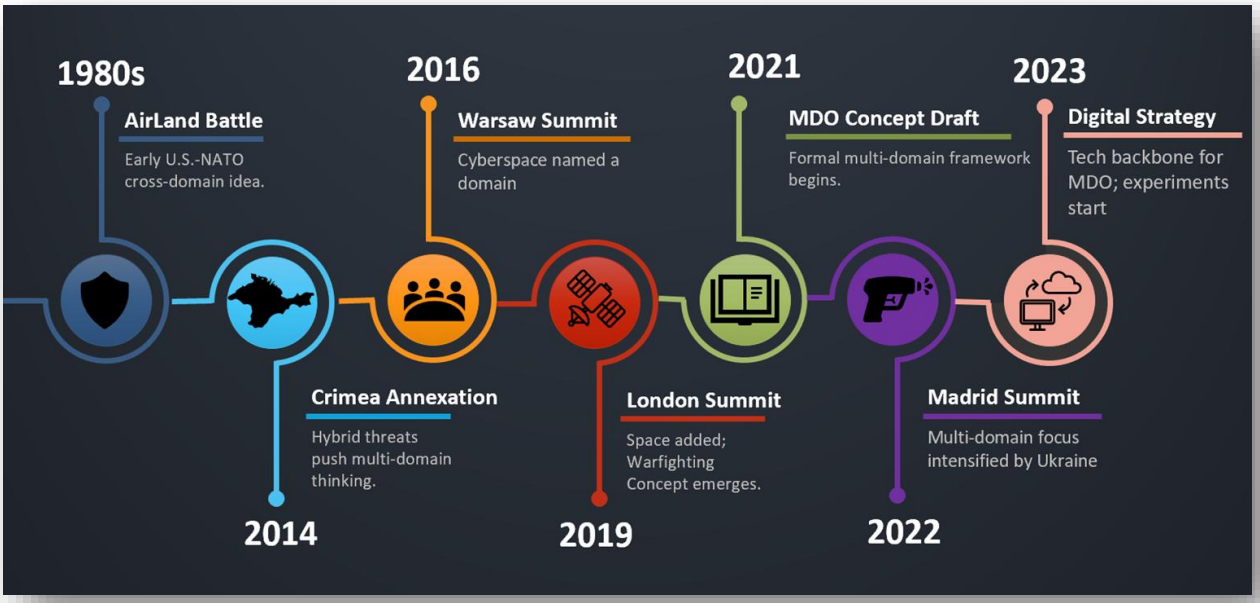



*Figure 5 Timeline of NATO-MDO*

NATO's path to adopting MDO closely followed these global doctrinal shifts but was also shaped by key geopolitical events and internal Alliance deliberations.

In 2014, Russia's hybrid tactics in the annexation of Crimea—including cyberattacks, disinformation, and irregular forces—highlighted the need for multi-domain awareness and response, prompting NATO to reconsider how it prepares for complex threats.

At the 2016 Warsaw Summit, NATO officially recognized cyberspace as an operational domain, a major step in adapting to new threat environments.

At the 2019 London Summit, NATO declared space as an operational domain, reinforcing its commitment to protect space-based assets and integrate space capabilities.

In 2021, NATO began drafting its own Multi-Domain Operations Concept, aligning with the evolving U.S. doctrine while tailoring it to the Alliance's collective defence approach.

In 2022, the Russian invasion of Ukraine became a real-time demonstration of multi-domain conflict, involving cyberattacks, information warfare, and conventional military force. This accelerated NATO's efforts to develop and operationalize MDO.

In May 2023, NATO formally published its MDO Concept, defining how the Alliance will synchronize operations across land, air, maritime, cyber, and space domains—along with non-military tools—to deliver coordinated effects.

Also in 2023, NATO adopted its Digital Transformation Strategy, providing the technological foundation—a secure, interoperable digital backbone—needed to support future MDO experimentation and implementation.

NATO's development of the MDO concept mirrors the broader global shift toward integrated, cross-domain operations. What began as a U.S. Army doctrinal evolution has now become a strategic imperative for the Alliance, ensuring that NATO remains agile, interoperable, and effective in an increasingly contested and multi-dimensional security environment.

**NATO Threat Assessment Relevant to MDO**

NATO's approach to Multi-Domain Operations (MDO) is shaped by a complex and evolving threat landscape characterized by state and non-state actors who increasingly operate across physical and non-physical domains. As stated earlier these threats are:

-Russia – A Direct and Immediate Threat

-Terrorist Organizations – Persistent Asymmetrical Threats

-Hybrid Threats – Blurring the Lines Between Adversaries

-China – A Strategic Challenge: The concept of "Multi-Domain Precision Warfare"

NATO's latest strategic and doctrinal documents—collectively recognize that today's threats—whether from near-peer competitors, terrorist organizations, or hybrid actors—require a multi-domain mindset and an integrated strategic response. MDO is therefore a critical enabler for NATO to deter, defend, and prevail in a contested and interconnected global environment.

**What MDO Is and What It Is Not?**

Multi-Domain Operations (MDO) is a modern military and strategic approach designed to meet the demands of a complex, interconnected battlespace. It goes far beyond traditional joint or combined warfare by integrating not just forces, but effects, timing, and decision-making across all operational domains.

At its core, MDO is a convergent strategy that seeks to create cross-domain synergy. By synchronizing actions across domains in real time, MDO generates tempo, agility, and pre-emptive advantage, allowing NATO or national forces to seize and maintain the initiative in fast-moving crises and conflicts.

A defining feature of MDO is its continuous and dynamic nature. It enables forces to act before adversaries can effectively respond, disrupting their decision-making cycles and presenting them with multiple simultaneous dilemmas.

Moreover, MDO fully incorporates cognitive warfare as a core element. It's not just about physical domains; influencing perception, shaping the information environment, and degrading adversary morale and cohesion are as crucial as kinetic actions.

However, it's equally important to understand what MDO is not:

- MDO is not just "multi-service" or joint warfare. That concept—commonly known as Joint All-Domain Operations (JADO)—focuses on cooperation among services. MDO goes further, focusing on effects integration across domains and functions, often blending military and non-military tools in real time.

- MDO is not linear or sequential. It is not about operating in one domain after another. Instead, it seeks to operate simultaneously and unpredictably, disrupting the adversary's ability to understand, plan, and react.

- MDO is not just about adding cyber or space to existing operations. True MDO involves full integration of all domains so that actions in one domain deliberately support and enable effects in others.

- MDO is not purely military. It acknowledges the critical role of non-military instruments of power—diplomatic, informational, economic, and technological—and emphasizes the importance of civil-military interoperability. This makes MDO a whole-of-government and, in NATO's case, a whole-of-Alliance endeavour.

**How MDO Fits into Counter-Terrorism and Hybrid Warfare**

Although MDO were initially conceptualized to address the challenges posed by near-peer adversaries and challenges—such as Russia and China—they have become increasingly relevant in the context of counter-terrorism (CT) and hybrid warfare. Originally, MDO was designed to enable military forces to achieve overmatch by integrating effects across all operational domains in a synchronized, and continuous manner. The aim was to counter technologically advanced opponents capable of denying access and operating in multiple domains simultaneously.

However, the nature of contemporary threats has evolved. Terrorist organizations and their state sponsors or enablers are increasingly behaving as hybrid actors, leveraging elements of multi-domain warfare to pursue their objectives. While they may not possess advanced conventional forces, they exploit asymmetric tools and tactics across several domains, often in a decentralized, adaptive, and cost-effective way. These include:

- Cyber operations, used to hack, disrupt, or manipulate,

- Information warfare, through propaganda, recruitment, and disinformation on social media,

- Use of commercial technology such as drones, encrypted communications, and dark web platforms,

- Collaboration with state actors for logistics, training, or protection,
- Grey zone tactics, operating below the threshold of conventional armed conflict to avoid attribution or escalation.

This evolution has blurred the line between conventional and irregular conflict. Terrorist groups are no longer confined to localized insurgency tactics; they are part of a broader hybrid threat landscape that spans borders, domains, and instruments of power.

There are already several examples of terrorist or proxy groups using MDO-like methods. Non-state actors have demonstrated the use of drones, electronic warfare, and psychological operations, often with support from states in the Middle East. DAESH conducted high-intensity urban warfare while also running a global online propaganda and recruitment campaign, using encrypted communications and satellite access. Russian-backed proxies in conflict zones like Ukraine use a mix of cyber, electronic warfare, drones, and disinformation, often blurring the line between state and non-state action.

Although these groups do not conduct full-scale MDO like a state military would, their ability to operate across multiple domains simultaneously presents a significant challenge. For this reason, MDO concepts are increasingly relevant to counter-terrorism strategies. NATO and its partners must consider terrorism not just as a military or intelligence issue, but as a multi-domain problem that requires coordinated responses across cyber, space, information, and traditional military domains.

Terrorist organizations themselves are increasingly adopting MDO principles, albeit in a more decentralized and adaptive manner. By exploiting digital tools, drones, and global financial networks, they operate across multiple domains to magnify their impact beyond traditional insurgency tactics. What makes this even more dangerous is the convergence between state-backed near-peer adversaries and non-state terrorist actors. When these groups collaborate—whether through direct sponsorship, shared technologies, or aligned strategic objectives—they create a hybrid threat that is far greater than the sum of its parts. This blurring of lines between state and non-state actors underscores why NATO must treat counter-terrorism as an integral component of Multi-Domain Operations, not as a separate or secondary concern.

**How NATO's CT Capabilities Must Evolve to Support MDO**

NATO must transform counter-terrorism (CT) from a reactive, standalone mission into a fully integrated enabler of **Multi-Domain Operations (MDO)**. Terrorist and proxy actors now exploit cyber, space, and the information environment, often with state backing, making CT central to Alliance resilience.

- **Intelligence-Driven CT:** NATO should harness AI, big data, and predictive analytics to fuse ISR from all domains, enabling early detection and rapid disruption of terrorist activity.
- **Integrated Mission Role:** CT must directly support NATO's counter-hybrid strategy by undermining terrorist networks, proxies, and influence campaigns that near-peer adversary's exploit.

- **Adapted Force Structure:** Special operations and CT units need organic cyber, EW, and space integration teams to operate across physical and digital domains.
- **Realistic Training:** Scenario-based exercises must reflect CT as part of coordinated MDO campaigns, preparing NATO forces for complex, hybrid conflicts.

In conclusion, Multi-Domain Operations (MDO) represent a transformative approach to modern conflict, enabling NATO to operate seamlessly across land, air, maritime, cyber, and space domains while synchronizing military and non-military instruments of power. In the context of counter-terrorism, the increasing sophistication and multi-domain capabilities of terrorist and proxy actors underscore the necessity of integrating CT into the MDO framework.

## *Session 5. CT Training in MDO Concept*

- ***Key Insight:*** *Current exercises are conventional, overlooking irregular terrorist tactics.*
- ***Policy Takeaway:*** *Scenario-based training is essential for resilience against hybrid terrorism.*
- ***Operational Implication:*** *Integrate cognitive defence and financial intelligence into training curricula.*
- ***Future Priority:*** *Build modular training packages (kinetic + cyber + information) for NATO CT exercises.*

# Integrating MDO into COE-DAT Education and Training Activities

*Dr. Zeynep SÜTALAN – COE DAT Academic Adviser*

**Introduction**

NATO Strategic Concept of 2022 defines terrorism "in all its forms and manifestations" as: "the most direct asymmetric threat to the security of our citizens and to international peace and prosperity." Terrorist organizations have evolved beyond the traditional battlefield, leveraging range of domains from physical to cyber for the aim of pursuing strategic effects disproportionate to their size. While NATO has adopted Multi-Domain Operations (MDO) concepts to prepare for peer and near-peer competition, these frameworks have not been fully integrated into counter-terrorism (CT) education and training. Doing so would close a critical capability gap, enhance interoperability, and ensure NATO forces are prepared for the hybrid, cross-domain character of terrorist threats.

**The Challenge: Terrorism as a Multi-Domain Phenomenon**

Terrorism has become a fluid, multi-domain challenge. Terrorists and terrorist groups are part of a broader hybrid threat landscape that spans borders, domains and instruments of power. They are already using multi-domains and sometimes they combine urban warfare, IEDs, cyber-attacks and real-time propaganda.

We all know the implications of the terrorist threat in physical domains, but today the terrorist threat got more complicated with commercial availability of drones to terrorists A number of groups has also incorporated Unmanned Arial Systems (UAS) in their terrorist campaigns. Terrorist groups such as Daesh, Al-Shabaab, Al-Qaeda in the Arabian Peninsula (AQAP), and Boko Haram are known to have varying levels of UAS capabilities and use the technology for intelligence, attacks and communication. The war in Ukraine has demonstrated to terrorists the potential of drones for ISR (intelligence, surveillance, and reconnaissance) and psychological operations, and how they can be easily deployed with AI capabilities.

Besides, today we know that that terrorists are very active in cyberspace. They are manipulating it for various activities propaganda and recruitment, fundraising, planning and coordination, intelligence gathering. With online radicalization, disinformation, and propaganda, we see that the battle of ideas is as decisive as kinetic actions. Terrorists exploit encrypted communications and cryptocurrencies, requiring responses that cut across domains. Today we also know that terrorist capabilities might be limited in the space domain, but they exploit commercially available satellite services they may use or using satellite imagery for operational

planning, they may spoof GPS signals (to mislead military navigation) or use satellite communications to coordinate attacks and spread propaganda securely.

**Why CT should be designed as a Multi-Domain Operation?**

First and foremost, terrorism as a threat is cutting across multiple domains. Therefore, the response to the terrorist threat should include integration of multiple domains. And thinking the agility of the threat, this integration is a requirement. Additionally, NATO's Warfighting Capstone Concept emphasizes cross-domain integration and multi-domain operations as the future of operations and extending this to CT is logical and in line with NATO's strategic priorities. For that reason, designing CT as an MDO is not a question of if but when for NATO. Since the concept of MDO and its translation to reality is ongoing, policies should think of including CT as one of the MDOs.

**Applying MDO to CT Training**

Understanding the multi-domain battlefield is essential for adapting counter-terrorism to contemporary threats. Accordingly, introducing the rationale and the mind set of MDO is the first critical objective that CT training should be aiming to achieve. MDO integrate actions across cyberspace, the information environment, and the physical domains of land, sea, and air, emphasizing their interconnected nature. Terrorist groups have increasingly exploited these overlaps. For example, using online platforms to amplify propaganda and coordinate logistics that manifest in physical attacks. To comprehend counter-terrorism operations as a form of MDO, NATO must identify the specific requirements for integrating intelligence, cyber capabilities, information dominance, and conventional force measures. This entails addressing gaps in interoperability, command-and-control, and legal frameworks that hinder effective coordination. More broadly, NATO faces the dual challenge of achieving MDO across all mission sets while tailoring it to the unique dynamics of counter-terrorism, where adversaries deliberately operate in the seams between domains and between military and civilian spheres.

**Integrating MDO into COE-DAT Education and Training Activities**

Centre of Excellence Defence Against Terrorism (COE-DAT) is the Department Head for NATO's defence against terrorism related education and training activities. In this respect, in line with NATO requirements COE-DAT should align its education and training activities. An initial endeavour should focus on integrating lectures into relevant courses to introduce the MDO mindset and promote awareness among practitioners and students. This stage should also spark discussions on the relevance of MDO to counter-terrorism and how it can be meaningfully integrated into NATO's approach. Subsequent efforts, aligned with the evolution of NATO's MDO concepts and doctrine, could include the use of hypothetical scenario-based tabletop exercises within existing courses, the creation of a dedicated new course on MDO and CT, and the gradual transformation of broader course content to reflect the MDO framework.

The courses relevant to the integration of an MDO approach into counter-terrorism include the Defence Against Terrorism Course, the Efficient Crisis Management (CM) to Mitigate the Effects of Terrorist Activities Course, the Terrorist Use of Cyberspace in General Terms Course, and the Basic Critical Infrastructure Security and Resilience Against Terrorist Attacks Course.

**Defence Against Terrorism (DAT) Course**

DAT is a generic course conducted by COE-DAT. Its primary aim is to provide participants with an awareness of the terrorist threat with its various dimensions (i.e. origins, root causes, tools, ideologies and motivations, etc.), to develop understanding of counter-terrorism in national and international contexts, to discuss these issues through a working group exercise.

The first step that the Centre could take to integrate MDO is to include one or two introductory lectures defining MDO, outlining its evolution, and explaining its adaptation within NATO, including its associated challenges and opportunities. This can be followed by illustrating terrorist activities as a multi-domain challenge by leading to the discussion of how CT can be conceptualised and designed as an MDO-enabled approach. Framing CT through an MDO lens will entail consideration of enhanced Intelligence, Surveillance and Reconnaissance (ISR), integrated Command and Control (C2), precision targeting and kinetic operations, influence operations, psychological operations, information operations, border security, cyber defence.

**Efficient Crisis Management to Mitigate the Effects of Terrorist Activities (ECMMETA) Course**

ECMMETA aims to provide participants with an understanding of the key elements of crisis management within the context of counter-terrorism, including preventative measures, first-response processes, risk reduction, and risk mitigation, as well as insight into controlling and countering narratives during and after a crisis. Within the scope of this course, MDO can be presented as an enabler across all stages of crisis management (CM) cycle such as enabling early detection, accelerating interagency preparedness, supporting real-time multi-domain response, and aiding recovery of information and infrastructure post-crisis. The course can include case studies, either real-world examples or hypothetical scenarios to discuss how to operationalize MDO before and during terrorist attacks.

**Terrorist Use of Cyber Space in General Terms (TUoCS) Course**

TUoCS Course intends to inform participants about key developments and emerging threats in terrorists' use of cyberspace and how cyberspace is used to support terrorist acts, enabling NATO and its partners to better anticipate and prepare for current and future challenges. From an MDO perspective, two lectures can be integrated to the course program. The first one can explore cyber as an enabling domain that terrorists use for facilitating their operations in other domains such as radicalization and recruitment, fundraising, planning and

coordination and intelligence gathering and also cyber domain as a weapon that terrorists use for cyber-attacks on critical infrastructure, for information warfare, for data breaches and leaks.

A second lecture may focus on countering terrorist cyber activities with an MDO perspective based on cyber defence strategies including disruption of digital terror infrastructure, critical infrastructure protection, international, interagency and public-private cooperation, developing red-teaming and threat foresight labs, leveraging technology for detection and disruption of terrorist propaganda, exposing terrorist lies and contradictions, and engaging with at-risk audiences. Against this framework, the primary emphasis should be on the MDO-informed mindset which considers cyber space no more as an isolated domain. The policy implication of this will mean involving defence, civilian infrastructure, telecom, law enforcement, space and aviation agencies, and media regulation authorities. Thus, cyber defence strategies must be coordinated with physical security, space assets, information operations, and critical infrastructure protection.

**Basic Critical Infrastructure Security and Resilience Against Terrorist Attacks (BCISRATA) Course**

BCISRATE Course aims to provide a better understanding of how nations can build and maintain demonstrably effective national Critical Infrastructure Security and Resilience (CISR) programs in an increasingly complex threat and security environment by adopting a holistic, all-hazards approach. The course is focused on critical lifeline infrastructure and retains a basic focus on the terrorist threat. Within this framework, lectures adopting an MDO perspective should first focus on identifying the vulnerabilities against terrorist attacks with the increased digitization of critical infrastructure. Terrorist organizations increasingly exploit cyber tools to enable or amplify activities across other operational domains. Understanding these cross-domain linkages is essential for identifying vulnerabilities, anticipating attacks, and building integrated responses. Examples for terrorist threats from cyberspace that affect cross domains in relation to CISR may include disrupting essential services like power grids, water supplies, and transportation systems, threats to aviation infrastructure via cyber like jamming air traffic control systems, cyber terrorist threat to Automatic Identification Systems, GPS navigation, and cargo tracking. The cyber capability serves as a command, control, and coordination mechanism for terrorism on the ground. Such as the use of social media, messaging applications like Telegram, and WhatsApp, and encrypted platforms to plan, recruit, and coordinate ground attacks. Cyber surveillance and target acquisition via tools like Google Maps, Open-Source Intelligence (OSINT) can also be included among them. The use of cyber means to disrupt emergency services, e.g., denial-of-service attacks during physical attacks can also be given as examples of utilization of cyber capabilities for conducting physical attacks.

Another lecture for integrating MDO perspective into CISR can focus on developing defensive, offensive and anticipatory strategies. Defensive strategies mentioning risk reduction,

threat mitigation, and system hardening across all domains and may include cross-domain threat detection and situational awareness, building redundant and diversified systems, hardening critical digital-physical interfaces and domain-specific hardening measures. Offensive strategies should underline active defence and disruption of threat actors before they strike. Conducting threat hunting, neutralization of malware, terrorist networks online to disrupt terrorist acts in the planning phase can be counted among the offensive strategies. These strategies can also include active disruption of terrorist coordination across domains such as degrading or blocking terrorists' ability to coordinate attacks using jamming, DDoS, or legal takedowns in order to prevent simultaneous, multi-domain attacks. In a similar vein, anticipatory strategies may include foresight, adaptation, and resilience building before terrorist attacks. These may involve using predictive analytics, scenario planning, and red-teaming to identify emerging terrorist threats. AI-driven threat forecasting, interagency and public-private wargaming, developing legal frameworks for anticipatory interventions can also be discussed within the framework of the anticipatory strategies.

**Conclusion**

Integrating MDO perspective into counter-terrorism education and training is a strategic necessity given that the threat of terrorism already spans borders, domains, and instruments of power. To be effective, counter-terrorism policies and operations must account for these cross-domain dynamics, recognizing how adversaries exploit both the physical and virtual environments simultaneously. Moreover, MDO is not solely about coordinating military domains; it also requires the integration of non-military instruments of power, which are central to whole-of-government and whole-of-society approaches. Only by aligning military, political, economic, and informational tools can NATO and its partners build a truly comprehensive counter-terrorism posture. COE-DAT as a NATO-accredited centre of excellence is committed to this end and plans to realize its commitment by including lectures on MDO in its four NATO accredited courses, the content of which are discussed above.

# The Role of Wargaming in CT Training within the MDO Framework

*Assoc. Prof. Emrah ÖZDEMİR – Turkish Military Academy*

In the context of evolving threat environments and the increasing complexity of Multi-Domain Operations (MDO), wargaming has emerged as a critical pedagogical tool in Counter-terrorism (CT) education and training. COEDAT recognizes wargaming not merely as a simulation exercise, but as a structured analytical method that enhances strategic foresight, operational planning, and decision-making under uncertainty.

Contemporary terrorist threats exploit domain convergence—leveraging cyber capabilities, information warfare, and transnational networks to challenge conventional security paradigms. Within this dynamic landscape, CT practitioners must be equipped to anticipate, adapt, and respond across all operational domains. Wargaming provides a controlled environment to test doctrinal assumptions, evaluate interagency coordination, and rehearse responses to complex, multi-domain terrorist scenarios.

Aligned with COEDAT's commitment to doctrinal integrity and interoperability, the integration of wargaming into CT curricula fosters critical thinking, red teaming, and scenario-based learning. It enables participants to engage with realistic threat vectors, assess cascading effects, and refine operational concepts in line with NATO standards.

The following sample wargame implementation—developed by Col. (R) Eray Ekin, Col. (R) Alper Aşkın, and L. Berke Çaplı—demonstrates a tactical-level approach to CT training in the MDO environment. Conducted with 20 participants, including military officers, academic scholars, and civilian security experts, the exercise was designed to simulate a localized terrorist threat scenario requiring immediate operational response.

Participants were presented with a concise tactical vignette and asked to respond to a set of structured questions within a 10-minute timeframe. These questions focused on threat assessment, force deployment, interagency coordination, and domain-specific considerations. The format emphasized rapid decision-making, doctrinal alignment, and the ability to synthesize multi-domain factors under time pressure.

This implementation serves as a practical and scalable model for CT education, reinforcing NATO principles while fostering interdisciplinary engagement and operational agility in the face of evolving terrorist threats.

# Operation Unseen Corner:
# Siege of Karsun Tactical Decision Game Version

*By Capt. (N) (R) Eray EKİN, Capt. (N) (R) Alper AŞKIN, L. Berke ÇAPLI - Radius Defence Wargame Domains*

**Situation**

You are the commander of a NATO-led Joint Task Force deployed near the harbour city of Karsun, a strategic chokepoint in a fragile state wracked by ethnic divisions and hybrid conflict. It is 1500 hours. Your force is tasked with ensuring humanitarian corridors remain open and secure while delivering urgent aid. A hostile, RED-aligned militia, backed by covert state support, contests your presence with advanced asymmetric tactics across land, sea, air, cyber, and space.

**At present:**

A battalion of your Commando Brigade secures the port, unloading food and medical supplies. Maritime Task Group (LPD + 3 FFGs) holds station offshore.

RED FPV drones and MANPADS teams operate in nearby districts. Cyber Defence reports malware disrupting port logistics and delaying aid. Refugee unrest grows at a major camp under RED-aligned criminal control. ISR detects RED loitering drones inbound toward evacuation routes, ETA 1800.

**Assets Available**

Land: 1 Commando Brigade (3 battalions, support), 1 Mechanized Battalion in reserve

Maritime: 1 LPD (6 assault helos, 4 multipurpose helos), 3 FFGs

Air: 2 F-16 squadrons (20 aircraft), UAV squadron, 1 ISR squadron (F-4)

Air Defence: 2 Patriot battalions, 1 SAMP battalion

Cyber/Space: 3 Cyber Defence Teams, 1 Cyber Offence Team, Space ISR Company

**Current Threat Indicators**

RED militia with MANPADS, FPV drones,

ATGMs in contested urban areas,

Spoof towers jamming comms, disguised as aid vehicles,

Loitering drones targeting convoys,

Civilian protests escalating at refugee camp,

Satellite ISR blackout possible due to external jamming.

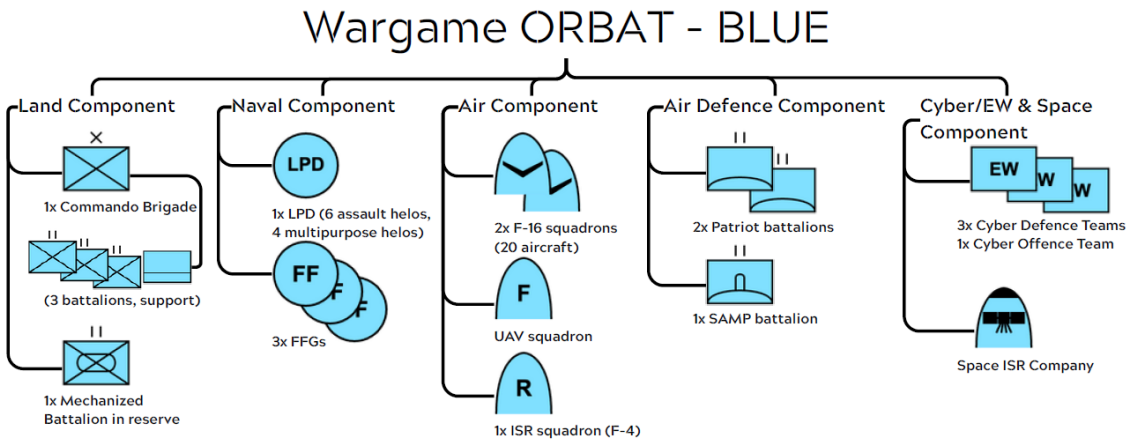
**Requirement**

You have 10 minutes to issue orders to subordinate commanders. Provide a fragmentary order with:

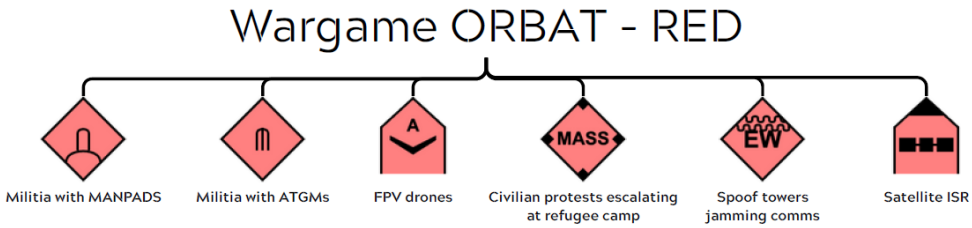
Scheme of manoeuvre (land, sea, air, cyber/space),

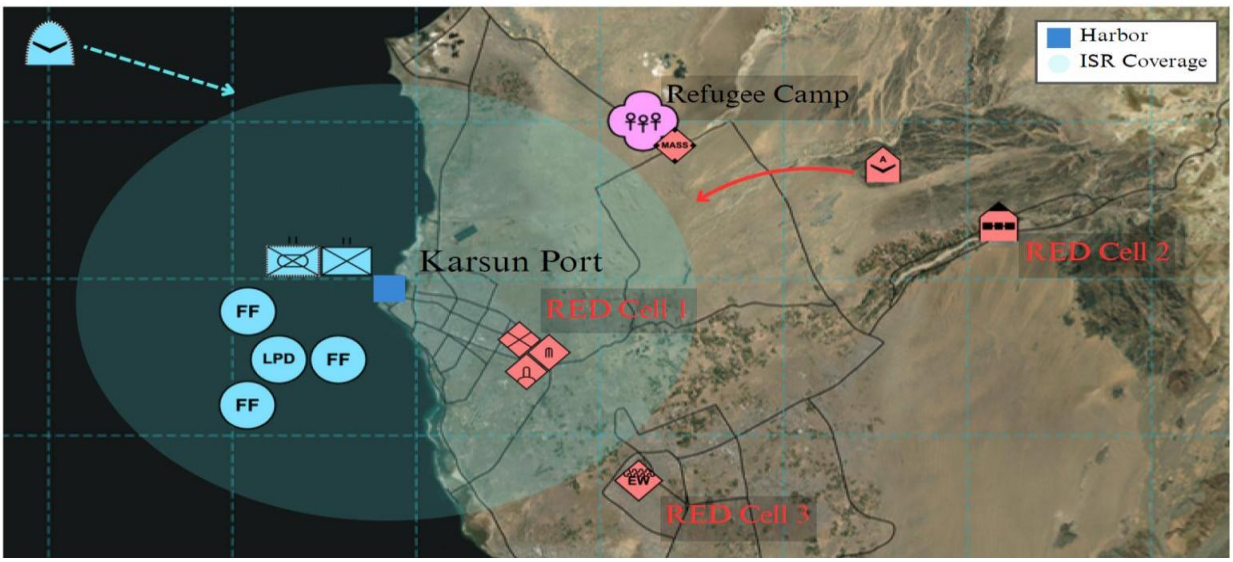
Priorities for humanitarian aid and civilian protection, Measures to counter RED hybrid threats.

What do you do, General?




**Any unit not displayed in the map is assumed to be on the harbour.*



**Consider while answering:**

What is the definition of your mission? e.g., Secure and hold the camp to ensure safe operations.

What is your concept of operations? e.g., Deploy ground forces, establish presence, and escort a convoy to the refugee camp.

What are your tasks to your subordinate units? e.g., Combat Elements: seize/hold camp, Security Elements: protect convoy en route.

**Example Answer:**

1500–2000: secure Karsun port and run two humanitarian corridors (camp/hospital) to deliver life- saving aid and protect civilians.

Land holds the port, clears/guards' routes, and keeps a QRF; mech reserve escorts and interdicts; maritime screens and provides CASEVAC; air maintains CAP/ISR and strikes time-sensitive drone/launcher threats under ROE; Patriot/SAMP layer C-UAS; cyber/space harden comms (PACE) and neutralize spoof towers with commercial/SAR backup if blackout.

Triggers: pause convoys under drone threat and engage C-UAS/EW; de-escalate camp unrest with KLE/non-lethal.

End state: corridors flowing, port normalized, drone threat suppressed, civilians protected.

**Tactical Wargame After Action Report**

*Facilitator & Annalists: Harun Raşit Yarar & Ada Sayın*

**Analysis introduction**

This wargame examined how participants react to evolving hybrid and cross domain threats. It focused first on immediate perceptions, that is, what we identify as the most urgent dangers when we encounter a crisis with limited information.

Next, the exercise explored how intuition and partial knowledge shape attention. In a short timeframe participants had to choose which unseen risks to prioritise and which objectives to pursue while operating under uncertainty.

The third aim was to map what participants treat as primary targets and achievements, and to identify the areas we tend to overlook.

Finally, the wargame aimed to test whether participants moved beyond joint operation mind set to true multi-domain synchronization. In other words, do we coordinate land, sea, air, cyber and space effects under a single plan to produce superior outcomes, or do they remain domain siloed?

By comparing first impressions, priorities and omissions, the exercise assessed whether participants share a common picture, and whether information gaps are complementary or recurrent across the group. The findings aim to help the workshop develop priority recommendations for adapting NATO's counter-terrorism doctrine, training and capabilities so those gaps are closed and resilience across all domains is strengthened.

**Questions to Consider**

Did responses achieve true multi-domain synchronization or remain domain siloed? Were there any telltale signs of tunnel vision, and were any red threats neglected? What critical capabilities are missing from the blue force?

Would more time or expert personnel fix the gaps, or do we need changes in doctrine, functions of authorities and training?

| Summary Table | |
|---|---|
| **Perceived Primary Red Threats** | **Unaddressed Red Capabilities** |
| a. **FPV / loitering drone swarms**<br>b. **MANPADS against helicopters and airlift**<br>c. **Cyber-attacks on port logistics and communications**<br>d. **Civilian unrest and RED control of the refugee camp**<br>e. **ATGMs and urban anti-armour fires** | a. **Dispersed FPV launch nodes and launch-site resilience**<br>b. **Sustained cyber-offensive capability against RED**<br>c. **Counter-disguise / vetting of aid vehicles and convoys**<br>d. **Indirect fire / stand-off rocket/artillery fires from depth**<br>e. **Complex information operations (targeted influencer ops by RED)** |

**Patterns in Answers:**

Humanitarian corridors and civilian protection are top priority

- Nearly every player framed the mission around keeping corridors open and protecting refugees

Strong emphasis on counter-drone (C-UAS), EW and cyber

- More than half explicitly prioritised drone mitigation, EW or cyber measures

ISR / persistent overwatch is repeatedly invoked

- UAV/space/shipborne ISR is commonly proposed for cueing and situational awareness

Civil-military, IO and negotiation are recognised but under-applied

- Several players (fewer than half) explicitly ask for negotiators, crowd/riot control and targeted

Divergence in risk appetite / legal caution

- Civilian responders lean toward non-lethal, intel, social measures and naval/evac priorities; military responders tend to offer direct kinetic tasking and explicit unit allocations.

Least Focused Areas in Answers:

Rules of engagement, legal constraints and escalation control

- Few players specified legal clearance, positive ID procedures or explicit escalation triggers.

Logistics, sustainment and berth/throughput management

- Convoy tempos, medical reception capacity and port throughput sequencing were rarely detailed.

Urban Collateral-Damage Mitigation / Protection of Civilians in Dense Terrain

- Little detail on precise measures to avoid civilian casualties in narrow streets,

multi-storey buildings, and mixed-use zones where RED fighters hide among civilians.

Influence Mapping

- Dedicated civil-military plans (negotiators, vetted aid points, influencer targeting and pre-scripted messages) were underused despite the obvious need to counter RED control and propaganda.

Crowd Management and Non-Lethal Riot Control in Urban Settings

- Most players omitted detailed riot-control assets, scalable non-lethal options, and staging/holding areas for crowds in confined urban spaces.

EW/Cyber–Air Deconfliction and Urban Emissions Management

- Players proposed EW/cyber effects but rarely specified who authorizes emissions, how to deconflict EW with air AD and civilian comms, or how to limit urban radio/EM interference that can endanger friendly forces and civilians.

Backup ISR / Sensor Redundancy under Spoofing and Satellite Blackout

- Plans under-addressed how to re-establish timely ISR (commercial SAR, airborne sensors, human lookouts) when space and local sensors a*re jammed or spoofed.*

**Unified FRAGO:**

*Below is a consolidated FRAGO (Fragmentary Order) based on all player submissions. What, if anything, is missing, and what does this document convey about the group's approach?*

**MISSION**

Joint force secures Karsun Port and approaches, secures and holds the refugee camp, escorts humanitarian convoys, and enables orderly embarkation and evacuation while degrading RED drone, C2 and influence capabilities and minimising civilian harm.

**EXECUTION**

**Commander's intent**: Deny RED control of the port and routes, protect civilians and humanitarian flows, restore port throughput for evacuation, and posture for follow-on stabilisation with minimal escalation.

**Concept of operations (phased)**

***Phase 1 - Shape and protect, 0 to 12 hours***

- Establish littoral and air overwatch.
- Activate EW, cyber and ELINT hunt cell to disrupt RED drone C2 and locate emitters.
- Deploy route security and camp defence forces.
- Start civil military information and key leader engagement.

***Phase 2 - Seize and clear, 12 to 36 hours***

- Mechanized and commando forces clear Red Cell 1 and secure approaches.
- Commando brigade clears camp sectors once EW and air defence posture validated.
- Maritime group secures port side entrance; LPD provides medical reception and embarkation.

***Phase 3 - Consolidate and enable, 36 hours onward***

- Hand over to static defenders and resume controlled port throughput.
- Maintain ISR, EW pressure and civil affairs to prevent resurgence.

***Tasks to subordinate units***

- Port defence task force (1 battalion plus commando, mechanized held in reserve): secure port, protect berths, coordinate LPD offload.
- Camp defence battalion (two battalions): hold perimeter, control access, manage crowds, provide triage.
- Mechanized battalion (QRF): clear Red Cell 1, screen approaches, exploit or suppress

counterattacks.

- Commando brigade: urban clearing, protect staging areas, support nonlethal de-escalation.
- Maritime group (frigates and LPD): sea control, radar cueing, afloat logistics and medical reception.
- Air component (F-16 CAP and armed ISR): overwatch, counter UAS suppression, time sensitive strike under ROE.
- UAV squadron and ISR nodes: persistent reconnaissance, cue shooters, maintain sensor redundancy.
- EW element and ELINT SIGINT hunt cell: spectrum interdiction, TDOA/DF geolocation, coordinate suppression with cyber and fires.
- Cyber defence and effects teams: harden C2, isolate compromised nodes, degrade RED C2 where authorised; preserve forensic logs.
- Civil affairs, negotiator and IO cell: engage local leaders, manage vetted distribution points, run safe movement messaging.
- Medical, logistics and NGO liaison: triage, CASEVAC routes, LPD reception, prioritise vulnerable evacuees.

**CONTROL MEASURES**

- Publish and mark evacuation lanes and maritime pickup coordinates.
- Emission control table in JOC; all EW and cyber effects coordinated through JOC.
- Sensor redundancy: UAV, ship radar, expendable UAV caches, ground OPs, commercial imagery fallback.
- Reporting: SITREP every 30 minutes during active phases; immediate report on major contact, civilian mass movement or casualties.
- Convoy pause trigger: halt if credible inbound loitering drone ETA under 10 minutes or if C-UAS coverage lost.

**SUSTAINMENT**

Preposition forward logistics for fuel, ammunition, EW consumables, medical supplies, water and rations. LPD serves as afloat logistics and medical collection point. Prioritise resupply to port defenders, convoy escorts and maritime evacuation teams.

**COMMAND AND SIGNAL**

Joint Operations Centre (JOC) with direct links to EW, cyber, ISR, maritime, air and ground

leads. JOC manages emission control, target deconfliction and attribution collection. Embed cyber and ISR liaisons with port and camp leads. Use protected redundant communications; publish nets and backup frequencies and test LPI SATCOM, optical links and LOS mesh before execution.

**RULES OF ENGAGEMENT (RoE) AND CIVILIAN PROTECTION**

Use minimum necessary force consistent with ROE and international law. Positive identification required before lethal engagement where feasible. Prefer non-lethal options and crowd management. Riot control assets on standby under commander approval. Notify NGOs and host nation authorities of major EW or cyber effects when feasible.

**ATTRIBUTION AND FORENSICS**

Collect ELINT, SIGINT, imagery chains and cyber logs into a central forensic repository. Hunt cell to produce time stamped evidence packages to support attribution and escalation decisions.

**END STATE AND TIMELINE (PLANNING)**

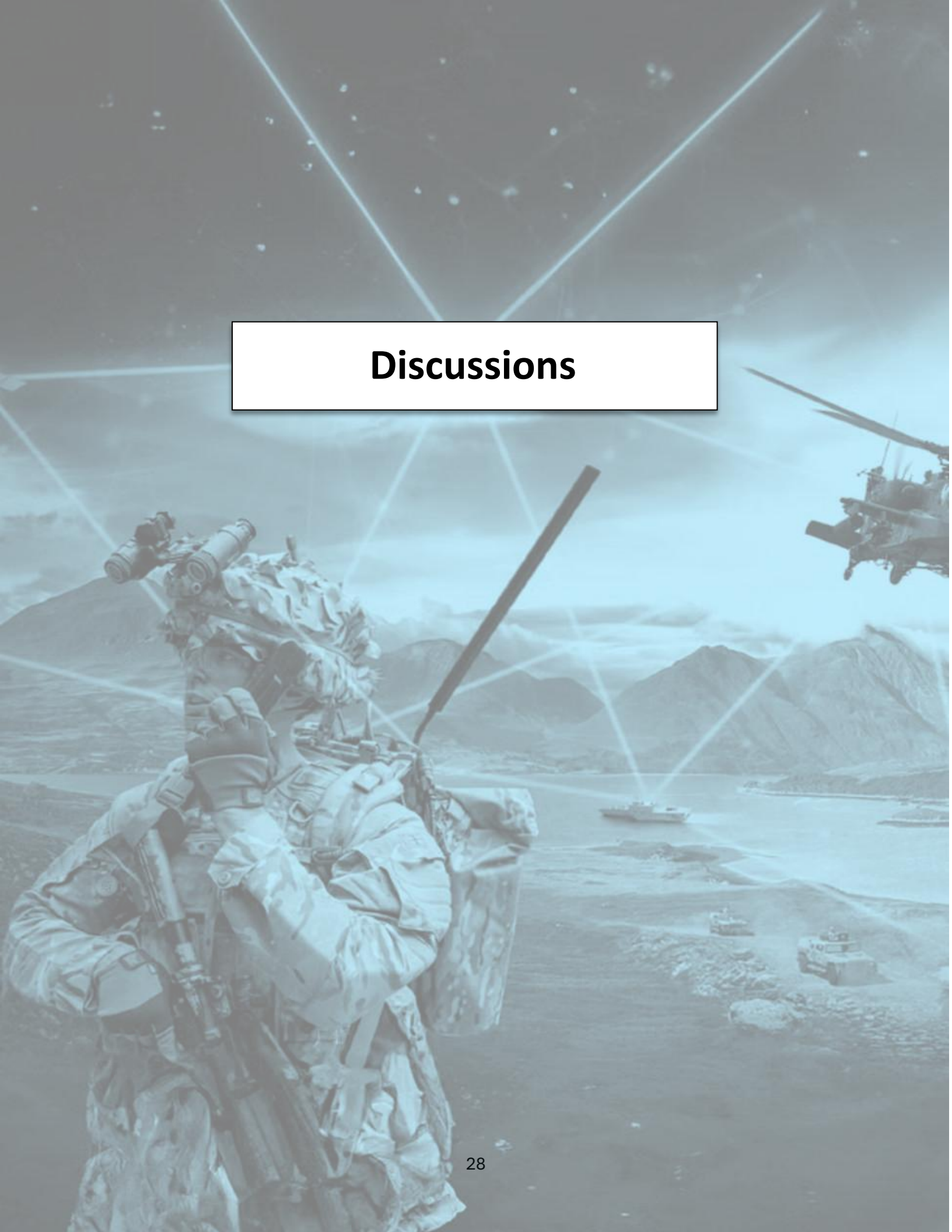
**End state:** LOCs and humanitarian corridors open and secure; port and embarkation functional; RED drone and cyber C2 degraded; camp stabilised; civilians protected; JOC holds a coherent multi-domain common operational picture.

**Timeline:**

H+0 JOC active, overwatch on station. H+4 logistics and pickup points ready. H+8-night unload window prepared.

H+12 mechanized clearing begins if EW/AD validated. H+24 convoy movement under escort if clearing confirmed.

H+36 to H+48 commando brigade secures camp sectors and embarkation intensifies.



# Discussions

# Introductory Note for the Discussion Sessions

The workshop devoted a significant portion of its programme to structured group discussions, designed to examine NATO's counter-terrorism (CT) posture in light of the emerging challenges of Multi-Domain Operations (MDO). This session sought not only to capture the perspectives of participants on specific thematic areas but also to stimulate forward-looking debate on NATO's doctrinal, institutional, and operational adaptation.

Each group was assigned a distinct focus area aligned with the overarching objectives of the workshop. Group 1 engaged in an in-depth analysis of doctrinal adaptation, assessing how NATO's CT framework could be recalibrated to respond more effectively to multi-domain terrorist threats. Their discussions highlighted issues such as the reactive nature of the Alliance's current posture, the insufficient integration of non-military instruments, and the urgent need to institutionalize NATO's CT role through permanent structures and systematic financial tracking. Group 2 concentrated on the capacity and training dimension. Their exchanges underscored gaps in NATO's collective education systems, the unevenness of national contributions, and the need to embed CT more systematically into Alliance-wide exercises and training curricula, with a particular emphasis on cooperation with civilian and local actors.

Despite these differences in emphasis, the groups were also guided by a set of common strategic questions. These included: How effective is NATO's current CT approach in an era of multi-domain threats? In what ways should MDO principles be integrated into NATO's CT doctrine and practice? And which investments represent the most urgent priorities for strengthening the Alliance's CT posture?

To capture the diversity and depth of these deliberations, this section of the report is structured in three stages. First, the results of each group's discussions are presented in dedicated subsections, highlighting their specific perspectives and recommendations. Second, a comparative analysis identifies the convergences between the groups, including shared concerns about NATO's reactivity, the lack of institutionalization, and the critical role of financial and cyber domains. Finally, the section synthesizes these findings into a set of overarching conclusions and recommendations, providing a coherent picture of the workshop's collective insights.

This structured approach ensures that the report not only reflects the richness of the debates but also distils them into actionable lessons for NATO's ongoing adaptation to the multi-domain threat environment.

# Cross-Cutting Strategic Questions for All Groups

**Synthesis of Group 1 and Group 2 Discussions**

**1. The Most Critical CT–MDO Coordination Areas**

Both groups converge on the view that intelligence and information-sharing remain NATO's weakest link. Group 2 emphasised the need to convert raw data into actionable intelligence with the help of AI and multi-actor exchanges, while Group 1 underlined the chronic underdevelopment of Alliance-wide sharing mechanisms. The synthesis is clear: NATO must move from episodic, minimal data disclosure to a culture of institutionalised intelligence integration that blends classified, OSINT, financial, and private-sector inputs.

Cyber and critical infrastructure protection were highlighted strongly by Group 2, and framed more broadly by Group 1 in terms of civil–military integration. Together, these perspectives underscore the necessity of protecting not only military assets but also energy grids, financial systems, and communication networks.

Civil–military cooperation and interoperability were identified as chronic challenges by both groups. Group 1 proposed a common institutional platform, while Group 2 focused on the operational obstacles of culture and law. The synthesis suggests NATO must establish a standing coordination mechanism to harmonise civilian, military, and private stakeholders across all Allies and Partners.

Both groups also pointed to societal and legal resilience. Group 2 emphasised proportionality under Article 5 and cognitive protection, while Group 1 warned of disinformation and attribution dilemmas. This indicates that NATO must treat the cognitive and legal space as part of the operational battlespace.

Finally, Group 1's insistence on financial tracking complements Group 2's stress on target analysis and early warning. The synthesis is that financial intelligence should be embedded in early-warning architectures, giving NATO predictive capacity.

**Key Takeaway**: NATO's critical CT-MDO coordination challenges are not merely technical but institutional. The Alliance must create a permanent, cross-domain coordination ecosystem that unites intelligence, infrastructure protection, societal resilience, and financial monitoring into a single framework.

**2. How Should NATO Counter MDO-Enabled Terrorist Groups?**

Group 2 advocated for clear threat definitions, prioritisation, and a network-centric approach, whereas Group 1 urged institutional innovation: permanent CT units, hybrid support teams, and specialised offices for cyber and finance.

Both groups agree NATO's current posture is too reactive. Group 2 highlighted the risk of Article 5 manipulation, while Group 1 noted NATO's dependence on national requests. The synthesis: NATO needs to shift from a posture of reactive solidarity to one of proactive anticipation, institutionalised at Alliance level.

Group 2's emphasis on strategic communication and cognitive defence complements Group 1's focus on urban cooperation and local partnerships. Taken together, NATO must defend not only territories but also populations and perceptions, strengthening ties with local authorities and communities while building capacity to counter extremist narratives.

**Key Takeaway**: NATO must combine operational agility (network-centric, rapid communication, cognitive protection) with institutional permanence (dedicated CT structures, financial and cyber offices, hybrid teams). One without the other risks either short-term agility without continuity, or structural strength without responsiveness.

**3. Priority Investments for Multi-Domain CT Capability Development**

Here the emphases diverge but are complementary. Group 1 viewed financial tracking as the structural prerequisite for all CT-MDO capability. Group 2 highlighted technological investments (space, unmanned systems, AI), training platforms, and civil–military–private partnerships.

The synthesis indicates that financial intelligence must be treated as the backbone of NATO's CT posture, but that backbone requires muscle and agility provided by new technologies, foresight platforms, and institutionalised partnerships.

Both groups stress the private sector's role: Group 2 identified specific industries (telecom, cyber, social media), while Group 1 called for a common platform. Combined, this means NATO must create formalised, standing partnerships with industry as part of its CT doctrine.

**Key Takeaway**: Investments must be dual-layered— (1) structural: financial intelligence, permanent CT units, interoperable frameworks; (2) enabling: emerging technologies, foresight mechanisms, and institutionalised partnerships with private and civilian actors.

**4. Overall Synthesis and Strategic Conclusions**

Taken together, the discussions of Group 1 and Group 2 paint a consistent picture: NATO's current counter-terrorism posture in the multi-domain era is fragmented, reactive, and overly conventional. Both groups diagnose the same vulnerabilities, albeit from different angles:

- Group 1 emphasises doctrinal and institutional adaptation: CT must be fully embedded in NATO structures, with permanent offices and multinational mandates.
- Group 2 emphasises operational agility and foresight: network-centric warfare adapted to CT, scenario-based training, cognitive defence, and technological innovation.

These perspectives are not contradictory but mutually reinforcing. Group 1 provides the architecture; Group 2 provides the dynamics.

***Strategic Synthesis for NATO*:**

1. **Institutionalise CT within NATO**: Establish permanent CT structures (financial and cyber offices, hybrid support teams, MDCT doctrine) to overcome episodic, reactive engagement.

2. **Recalibrate Training and Exercises**: Develop scenario-based, foresight-driven training that integrates OSINT, AI, and tailored programs for military, civilian, and private actors.
3. **Embed Financial Intelligence into Early Warning**: Treat financial flows as both a strategic lever and a predictive tool, linking them to broader situational awareness.
4. **Protect the Cognitive Domain**: Counter extremist propaganda, secure public trust, and maintain proportionality under international law to safeguard NATO's legitimacy.
5. **Institutionalise Civil–Military–Private Partnerships**: Formalise cooperation with tech companies, satellite operators, and local authorities through structured frameworks and common platforms.
6. **Balance Structural Permanence with Operational Agility**: NATO must simultaneously anchor CT within its doctrinal corpus and retain flexibility to adapt quickly to evolving terrorist tactics.

**Conclusion**

The synthesis of Group 1 and Group 2 makes it evident that NATO's future counter-terrorism posture must be both permanent and adaptive, structural and agile. Only by marrying Group 1's call for institutionalisation with Group 2's call for innovation and foresight can NATO transform CT from a reactive, nationally driven task into a core, multi-domain Alliance function. In the face of adaptive terrorist adversaries, anything less would risk leaving NATO strategically blind and operationally vulnerable.

| Cross-Cutting Question | Group 1 Emphasis | Group 2 Emphasis | Synthesis / Key Takeaway |
|---|---|---|---|
| **Most Critical CT–MDO Coordination Areas** | Alliance-wide intelligence sharing; civil–military integration; institutional platforms; disinformation dilemmas; financial tracking | Convert raw data via AI; infrastructure protection; cultural/legal obstacles; proportionality under Article 5; cognitive protection; target analysis | Institutionalized intel integration; protect infra; coordination mechanism; cognitive/legal as battlespace; embed financial intelligence |
| **How Should NATO Counter MDO-Enabled Terrorist Groups?** | Institutional innovation: permanent CT units, hybrid support teams, specialized offices; reliance on national requests | Clear threat definitions; prioritization; network-centric approach; risk of Article 5 manipulation; cognitive defence; local partnerships | Shift from reactive to proactive; combine agility (network-centric, cognitive defence) with permanence (dedicated CT structures) |
| **Priority Investments for Multi-Domain CT Capability Development** | Financial tracking as structural prerequisite; common platform for private sector cooperation | Tech investments (space, AI, drones); training platforms; civil–military–private partnerships | Dual-layered investments: (1) structural—financial intelligence, permanent CT units; (2) enabling—tech, foresight, partnerships |
| **Overall Synthesis and Strategic Conclusions** | Doctrinal and institutional adaptation; CT fully embedded with permanent offices & multinational mandates | Operational agility & foresight: network-centric CT, scenario-based training, cognitive defence, innovation | CT posture must be both permanent & adaptive: structural permanence + operational agility; institutionalization + innovation |

*Figure 6 Cross-Cutting Strategic Questions: Group 1 vs Group 2*

# Group 1: Strategic and Doctrinal Adaptation

**Background**

The discussions of Group 1 began from a strategic angle, questioning whether NATO's existing counter-terrorism (CT) framework is sufficiently robust to address threats that increasingly manifest across multiple domains. Rather than treating terrorism as a secondary concern compared to peer adversaries, participants emphasized the need to recalibrate Alliance doctrine. Their debate therefore concentrated on how NATO's conceptual foundations, institutional structures, and operational doctrines must evolve to embed CT as a core element of the Multi-Domain Operations (MDO) approach.

Participants consistently emphasized that terrorism, although historically framed and treated as a predominantly asymmetric phenomenon, is undergoing a profound process of transformation whereby its methods and modalities increasingly intersect with multi-domain features such as cyber warfare, financial manipulation, information operations, and the strategic use of new technologies. Against this backdrop, a central concern articulated by the group was the risk that NATO, in its understandable concentration on deterring and countering peer and near-peer adversaries, most notably the Russian Federation, may inadvertently relegate the terrorist threat to a position of secondary importance. Such a posture, it was argued, would create doctrinal and operational blind spots that adversarial non-state actors could exploit with potentially devastating strategic consequences. Accordingly, the discussions converged on the imperative that NATO's doctrinal framework must evolve to treat CT and MDO not as parallel but as deeply intertwined challenges, requiring an integrated and forward-looking adaptation of Alliance concepts, structures, and practices.

**In-Depth Discussion Questions**

**1. Effectiveness of NATO's Current CT Approach**

The group's deliberations revealed that NATO's counter-terrorism (CT) posture, while demonstrating certain strengths and partial effectiveness in specific areas, remains misaligned with the trajectory of future threats. Participants consistently emphasized that the Alliance has developed useful mechanisms for coordination, training, and strategic awareness, but these have not yet been systematically recalibrated to meet the challenges posed by adaptive terrorist organizations capable of operating across multiple domains. The result is a doctrinal architecture that appears robust on paper yet risks proving insufficient when confronted with the speed, innovation, and transnational reach of contemporary terrorist networks.

***Cyber, Space, and Information Environments.*** There was broad consensus that space, despite being an increasingly critical arena of great-power competition, is unlikely to emerge as a practical operational theatre for terrorist organizations in the near future, given the prohibitive technological and financial barriers. In contrast, the cyber domain was unanimously identified as the most pressing frontier. Terrorists' growing exploitation of cryptocurrencies, digital financial instruments, and cyber-manipulation tactics was described as a fundamental vulnerability for the Alliance. Participants highlighted the dual-use dilemma embodied in the observation that *the ability to defend effectively against cyber intrusions necessarily implies the*

*parallel development of offensive cyber capabilities.* This interdependence generates not only technical challenges but also ethical, political, and legal complexities for NATO. In addition, the rapid evolution of unmanned aerial systems, as evidenced by the Ukrainian case where drones are upgraded on an almost weekly basis, was cited as a demonstration of adversarial agility. Terrorist groups, while lacking state-level resources, could adapt similar patterns of technological innovation, forcing NATO to accelerate its responsiveness.

***Policy Provisions*.** Participants acknowledged that NATO has taken steps to incorporate multi-domain considerations into its broader security policies. Nevertheless, the so-called "underground dimension"—referring to subterranean, covert, and irregular activities often exploited by terrorist groups—was regarded as neglected. This dimension, encompassing both literal underground infrastructures (such as tunnels and hidden supply routes) and figurative ones (such as clandestine online networks), represents a doctrinal blind spot. Participants argued that this area requires explicit recognition as a new doctrinal frontier if NATO is to preclude operational surprises and sustain a credible counter-terrorism posture in MDO.

***Preventive Strategies.*** Perhaps the most significant critique was that NATO's CT efforts continue to be characterized by a reactive orientation, with engagement triggered primarily by national requests rather than by Alliance-wide foresight. Structural deficits in information-sharing persist, rooted in both political reluctance and technical incompatibilities among Allies. As a result, early warning remains fragile, and opportunities for pre-emption are routinely missed. Participants argued that preventive strategies must be redesigned to transcend mere reaction. They should be proactive, dynamic, and adaptive to the shifting priorities of different domains as well as the fluid transitions between peacetime, hybrid competition, and open conflict. In this context, building a culture of trust-based intelligence exchange, supported by adaptable early warning mechanisms, was deemed essential to strengthening NATO's resilience against multi-domain terrorism.

**2. Integration of MDO Principles into CT Approach**

The discussions within Group 1 underscored that integrating the principles of Multi-Domain Operations (MDO) into NATO's counter-terrorism (CT) posture requires not only technical and operational adjustments but also a deeper rethinking of the Alliance's doctrinal underpinnings. Participants framed the challenge as one of ensuring that NATO does not treat CT and MDO as parallel tracks, but rather weaves them into a coherent operational and strategic fabric. Four principles—unity, interconnectivity, creativity, and agility—were identified as the pillars upon which such integration must rest.

***Unity.*** Participants emphasized that achieving genuine doctrinal cohesion in CT requires Allies to share a common understanding of what terrorism constitutes in both its operational manifestations and its strategic implications. However, it was acknowledged that debates over definitional clarity have historically paralyzed international consensus, as prolonged negotiations over terminology often result in political deadlock. For this reason, the group recommended a functional approach: instead of seeking exhaustive legal definitions, NATO should focus on identifying and addressing the observable behaviours, tactics, and networks that constitute terrorist threats. Such a pragmatic stance would allow the Alliance to

sustain operational momentum without being hindered by unresolved semantic disputes. The emphasis was thus placed on building consensus around actionable threats and operational requirements rather than abstract conceptual debates.

***Interconnectivity.*** Effective integration of CT into MDO presupposes that NATO's information-sharing practices evolve far beyond the current model of fragmented and often superficial exchanges of raw data. Participants argued that what is urgently required is the institutionalization of mechanisms that enable the circulation of high-quality analytical products across the Alliance. This entails moving from a culture of minimal disclosure toward one of substantive collaboration, where intelligence is contextualized, synthesized, and oriented toward actionable foresight. Open-source intelligence (OSINT), if systematically collected and properly analyzed, could serve as a valuable complement to classified inputs, while private sector data—particularly from investment firms, financial institutions, and technology companies—could provide insights into patterns of economic and technological exploitation by terrorist actors. By cultivating such multi-source integration, NATO could significantly deepen its analytical depth, enhance situational awareness, and ensure that CT operations remain informed by a multi-domain perspective.


***Creativity.*** A recurrent theme was that terrorist organizations often conceptualize the battlespace in ways that differ markedly from NATO's conventional military logic. They adapt maps, exploit technology, and employ asymmetric tactics in unorthodox ways, frequently blurring the boundaries between physical and digital domains. To counter this adaptive mindset, NATO must cultivate creativity within its CT doctrine and avoid an overreliance on technological solutions alone. Participants warned that while advanced technologies such as

Artificial Intelligence (AI) are becoming increasingly influential, they must be embedded within frameworks that continue to privilege human judgment, intuition, and manual skills. Competencies such as traditional map-reading, human terrain analysis, and cultural understanding were described as indispensable for interpreting terrorist intent and behaviour. Long-term research and development, inspired by initiatives such as the European Union's Horizon program, was recommended to institutionalize innovation in CT-MDO and to sustain NATO's ability to anticipate rather than merely react to adversarial adaptations.

***Agility.*** Perhaps the most pressing concern raised was the risk that NATO's current strategic fixation on deterring Russia may result in a dangerous neglect of terrorism, particularly as non-state actors are predicted to regain prominence in the global threat landscape within the next five years. To guard against this, NATO must maintain a standing capacity for adaptability and agility in its CT forces. This means ensuring that Alliance structures are not rigidly locked into a singular strategic orientation but are capable of rapid adjustment to shifting threat environments. Flexibility in force composition, modularity in operational design, and responsiveness in command-and-control structures were all identified as necessary attributes of an agile CT posture. Furthermore, participants stressed the importance of refining NATO's legal and political mechanisms to ensure that such agile operations remain firmly anchored in international legitimacy. Without such legal grounding, NATO's ability to act decisively in multi-domain contexts would be vulnerable to contestation and delegitimization by adversaries.

**3. CT's Role in Shaping MDO Operational Art**

***Contribution to NATO Objectives.*** Participants underlined that counter-terrorism (CT) is not a peripheral task but one that contributes directly to NATO's overarching strategic objectives. By shaping adversarial behaviour, contesting activities in the grey zone, and deterring future threats, CT provides the Alliance with an indispensable set of instruments for maintaining credibility and cohesion. The group emphasized that these contributions should not remain implicit or ad hoc but must be formally codified within NATO's doctrinal corpus. Such codification would ensure that CT is systematically embedded in operational planning and recognized as an integral component of MDO rather than an afterthought.

***Strategic Tools.*** Several tools were highlighted as essential for embedding CT into the operational art of MDO. National special forces were described as critical assets, given their ability to operate with precision, flexibility, and speed across multiple domains. Intelligence networks, both national and multinational, were identified as the connective tissue that makes coordinated CT operations possible. Equally important are non-military instruments—such as financial sanctions, legal frameworks, and public diplomacy—which can constrain terrorist networks without recourse to kinetic force. Technological innovation, particularly in cyber defence and unmanned systems, was also stressed as a growing enabler. As a comparative example, the Regional Anti-Terrorist Structure (RATS) of the Shanghai Cooperation Organization was cited as a model from which NATO could draw lessons when considering how to institutionalize a dedicated CT body within its own framework.

***Information and Psychological Operations.*** The group also recognized that CT effectiveness depends not only on direct action but also on the ability to shape narratives and

perceptions. Psychological operations were highlighted as powerful indirect tools that can undermine terrorist legitimacy, disrupt recruitment, and counter extremist propaganda. The extensive use of such techniques by Russia was noted both as a cautionary example and as a source of insight: while adversarial exploitation of information environments demonstrates the risks, it also underscores the necessity for NATO to innovate doctrinally in this field. Participants stressed that embedding psychological and information operations into CT doctrine would provide the Alliance with a more comprehensive toolkit for countering multi-domain terrorist strategies.

**4. Legal and Political Frameworks**

***International Legal Constraints.*** Participants emphasized that international law continues to set the parameters within which NATO must operate, with *jus in bello* serving as the fundamental reference point for legitimacy. While NATO enjoys a degree of operational flexibility through its collective defence mandate, any action against terrorism in a multi-domain context often requires clear authorization from the United Nations Security Council to prevent challenges to legality and legitimacy. The absence of consolidated legal guidance was identified as a recurring problem, leading to uneven interpretations across Allies. To address this, participants proposed the development of a comprehensive legal reference document—potentially modelled after established instruments such as The Hague conventions—that would bring clarity and consistency to NATO's CT-MDO posture. Such a resource would serve both as a doctrinal anchor and as a practical guide for operational planning.

***Sovereignty and Intervention in Cyber/Space.*** Discussions revealed that sovereignty remains a sensitive and contested issue, particularly in relation to cyber and space domains. While NATO has established responsibility for cyber defence as a collective matter, the conduct of offensive cyber operations continues to be reserved for individual nations, reflecting both political sensitivities and legal ambiguities. This division creates potential operational gaps, as defensive measures are often insufficient without corresponding offensive capabilities. Space, by contrast, remains under-defined both legally and doctrinally. Participants observed that the absence of clear norms or agreed rules of engagement in the space domain creates uncertainty and risks leaving NATO unprepared should terrorists or state-sponsored proxies attempt to exploit emerging space-based vulnerabilities.

***National Policy Divergence.*** Finally, the group noted that one of NATO's most enduring challenges lies in the divergent approaches adopted by Allies in the field of counter-terrorism. Some member states continue to prioritize military instruments, while others rely heavily on law enforcement and judicial tools, and still others adopt a more restrained posture, abstaining from active CT engagement beyond their own borders. These differences create unevenness within the Alliance and open seams that terrorist actors can exploit to establish transnational networks and evade coordinated action. Achieving convergence on CT-MDO doctrine was therefore recognized as one of NATO's most formidable challenges. Without greater political alignment, NATO risks fielding an inconsistent response in which the sum of national efforts falls short of the collective requirements posed by multi-domain terrorist threats.

**Conclusion**

The deliberations of Group 1 made it evident that, despite incremental progress in recent years, NATO's counter-terrorism posture remains only partially aligned with the evolving realities of multi-domain terrorism. The Alliance's current approach continues to be shaped predominantly by a reactive orientation, triggered largely by national requests rather than by collective foresight. This orientation leaves NATO vulnerable to surprise and constrains its ability to shape the threat environment proactively. Equally, the reliance on national contributions, without the existence of permanent institutionalized counter-terrorism structures at the NATO level, perpetuates unevenness across the Alliance and prevents the consolidation of a truly collective CT-MDO framework.

In response to these challenges, the group identified several overarching imperatives that should guide the Alliance's doctrinal and operational adaptation:

***Institutionalization of NATO's CT Mandate.*** Counter-terrorism must no longer be regarded as a peripheral or nationally bounded issue. Instead, it should be elevated to a fully integrated NATO responsibility, complete with doctrinal development, dedicated training pathways, and the establishment of standing institutional structures. Only through such institutionalization can the Alliance move beyond an episodic, case-by-case approach and instead achieve predictability, continuity, and coherence in its CT posture.

***Comprehensive Multi-Domain Integration.*** The fight against terrorism in the MDO era requires the systematic alignment of military and non-military instruments. This includes the integration of civilian authorities, financial institutions, private-sector actors, and technological stakeholders into NATO's planning, exercise, and crisis management processes. By embedding such cross-sectoral cooperation into its doctrinal framework, NATO can ensure that terrorism is confronted as a multidimensional phenomenon rather than as a narrowly military problem.

***Proactive Investment in Capabilities.*** Participants highlighted the necessity of investing in capabilities that strengthen NATO's anticipatory posture. Persistent financial tracking, robust cyber defence mechanisms, and advanced intelligence-sharing arrangements were identified as priorities. These capabilities must be supported by sustainable financial commitments, institutionalized research centres, and innovation-driven partnerships that allow NATO to keep pace with the technological dynamism displayed by both state and non-state adversaries.

***Legal and Political Convergence.*** Finally, NATO must navigate the complex web of international legal frameworks with precision, while at the same time fostering political convergence among Allies. Divergent national approaches to counter-terrorism—whether military-centered, law-enforcement-driven, or abstentionist—create exploitable seams that adversaries can use to their advantage. Without greater convergence, NATO risks fielding a fragmented response in which national efforts fail to coalesce into an effective collective posture.

Taken together, these imperatives underscore that counter-terrorism can no longer be siloed or treated as an ancillary concern in an age where terrorist organizations have demonstrated the ability to exploit multiple domains simultaneously. While such organizations

may not possess the full spectrum capabilities of peer adversaries, their asymmetric, adaptive, and multi-domain strategies represent a direct and enduring threat to NATO's cohesion, credibility, and resilience. The conclusion reached by Group 1 was clear: only through doctrinal adaptation, underpinned by institutional innovation, political alignment, and strategic foresight, can NATO preserve its unity of effort and fulfil its mandate of safeguarding the security of its member states against the evolving spectre of multi-domain terrorism.

# Group 2: Capability and Training Development

**Background**

Group 2 approached the workshop's objectives from a practical and operational perspective, examining the concrete skills, capabilities, and training mechanisms NATO requires in order to remain resilient. Their focus was less on doctrine and more on the ways in which training design, exercises, and cooperation with civilian and private actors could be restructured. By addressing gaps in preparedness and interoperability, the group highlighted pathways for equipping personnel and institutions to confront terrorist organizations that exploit the multi-domain environment.

Participants highlighted that terrorism, far from being confined to traditional asymmetric tactics, is now intersecting with multi-domain features, ranging from cyber intrusions and the exploitation of digital finance to the manipulation of information environments and the low-cost use of unmanned systems. Against this backdrop, Group 2 emphasized that NATO risks falling into a doctrinal and operational trap: its training and exercises remain too conventional, and its cooperation with civilian and private actors is fragmented, leaving exploitable vulnerabilities.

Accordingly, Group 2's work focused on two broad lines of inquiry: first, how to restructure training and exercises to prepare for terrorist organisations that increasingly operate across multiple domains; and second, how to embed civil–military and private-sector cooperation into NATO's CT-MDO framework to ensure interoperability, legitimacy, and resilience.

**1. Restructuring Training and Exercises**

***Findings***

Group 2's analysis revealed that NATO's training and exercise architecture faces three structural challenges:

- **Conceptual Ambiguity**: The lack of a clear, shared understanding of what constitutes terrorism in a multi-domain context complicates exercise design. Key terms such as "terrorist," "non-state actor," and even "MDO" itself remain insufficiently defined.
- **Conventional Bias**: NATO's current exercises are heavily skewed towards kinetic, peer-adversary scenarios. This orientation does not adequately capture the hybrid and irregular methods of terrorist groups, which increasingly combine cyber operations, disinformation, and drone attacks.
- **Reactive Posture**: Exercises often replicate past or present threats rather than anticipate emerging ones. Terrorist organisations, with their rapid cycles of innovation, are able to exploit this gap.

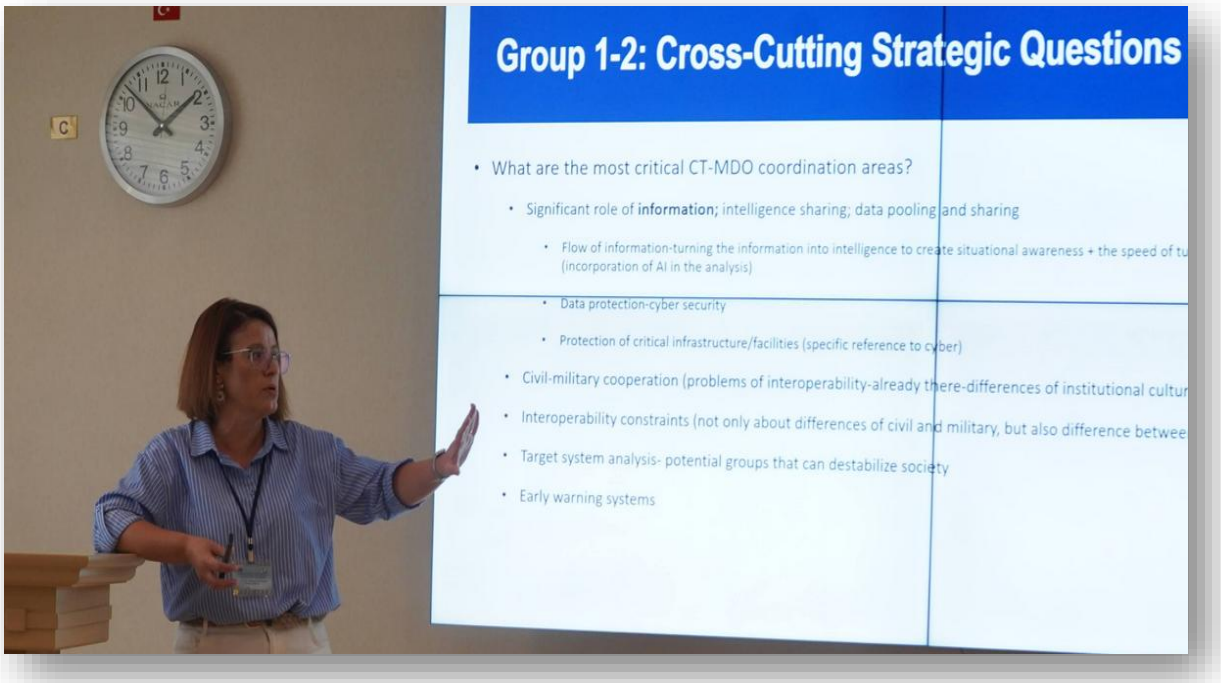
The group further observed that MDO in its present form is overly military in outlook, often neglecting the human and societal dimensions. While it theoretically integrates non-military instruments, in practice it remains closer to a digitalised extension of conventional warfare.

***Strategic Considerations***

Participants recommended a fundamental restructuring of NATO training to integrate multi-domain terrorist scenarios into exercises. This includes:

- **Scenario-based and live-synthetic training**: Exercises should simulate multi-domain terrorist campaigns that blend cyber, physical, and informational attacks.
- **OSINT integration**: Training should systematically incorporate open-source intelligence to reflect both the tools used by terrorists and the need for anticipatory situational awareness.
- **Strategic foresight**: Training must be future-oriented, incorporating trend analysis of terrorist tactics to feed into early warning mechanisms.
- **Audience-specific design**: Exercises should be tailored to the operational realities of different actors—military personnel, law enforcement, customs, and private stakeholders—while cultivating cross-domain leadership skills among CT leaders.
- **Dedicated doctrine**: Rather than retrofitting terrorism scenarios into an MDO framework, participants argued for the establishment of a Multi-Domain Counter-Terrorism (MDCT) doctrine, ensuring that training reflects the unique operational context of terrorism.

In sum, NATO's training architecture must evolve from conventional, reactive designs toward anticipatory, multi-domain, and multi-actor exercises that reflect the realities of contemporary and future terrorist strategies.



## 2. Civil–Military and Private Sector Cooperation

### *Findings*

Group 2 also focused on the indispensable role of cooperation between military forces, civilian authorities, and the private sector. The group identified four persistent barriers:

- **Legal and Regulatory Constraints**: National laws often restrict the extent of military support to law enforcement or limit information sharing, producing interoperability gaps.
- **Cultural Divides**: Military and civilian actors operate with different institutional logics, communication styles, and tempos, creating friction even when cooperation is legally permissible.
- **Underutilisation of Private Sector**: Telecommunications, satellite operators, and digital platforms hold capabilities central to counter-terrorism, yet NATO's engagement with them remains sporadic and ad hoc.
- **Cybersecurity Deficits**: Terrorists are increasingly exploiting cyber vulnerabilities, but NATO has yet to establish structured partnerships with cybersecurity firms.

The group also noted that these challenges extend across borders: differences between NATO Allies and Partners in legal frameworks, technical capabilities, and political will create additional seams that terrorists can exploit.

### *Strategic Considerations*

Group 2 emphasised that NATO must institutionalise civil–military and private-sector cooperation rather than treating it as an optional or supplementary dimension of CT-MDO. Recommended measures include:

- **Formal frameworks for joint planning and training**: Embedding civilian and private stakeholders into NATO's exercise cycles and decision-making processes.
- **Structured partnerships with technology and cybersecurity firms**: Establishing agreements that enable information sharing, digital monitoring, and rapid interventions against terrorist manipulation of cyberspace.
- **Adaptation of CIMIC principles**: Applying Civil–Military Cooperation doctrines to multi-domain CT operations, ensuring that civilians are not only protected but actively integrated into resilience strategies.
- **Cross-sector interoperability**: Developing protocols to bridge cultural and institutional divides, thereby ensuring smoother coordination in times of crisis.

By embedding these partnerships into doctrine and practice, NATO would both strengthen operational effectiveness and reinforce its legitimacy in the eyes of member states and global partners.

**Conclusion**

Group 2's deliberations made it evident that NATO's posture against multi-domain terrorism will remain insufficient unless it recalibrates its approach to **training** and **cooperation**. The Alliance must acknowledge that terrorism today operates across domains and thrives in institutional seams.

Three overarching imperatives emerged:

1. **Restructuring Training**: NATO must move beyond conventional, reactive exercises and adopt a forward-looking MDCT training doctrine. This doctrine should integrate scenario-based simulations, OSINT, strategic foresight, and tailored exercises for military and civilian actors alike.
2. **Institutionalising Cooperation**: Civil–military and private-sector partnerships must be embedded through structured frameworks, cybersecurity alliances, and adapted CIMIC principles, ensuring that all relevant actors are prepared for multi-domain CT.
3. **Embedding Legitimacy and Resilience**: CT operations must protect civilian populations, preserve proportionality under international law, and safeguard cognitive resilience against extremist propaganda.

Taken together, these imperatives underline that counter-terrorism cannot be an afterthought in NATO's MDO posture. A dedicated MDCT framework, built upon training reforms and institutionalised partnerships, is essential if NATO is to anticipate and outpace the evolving strategies of multi-domain terrorist actors.

| Category | Group 1 | Group 2 | Synthesis |
|---|---|---|---|
| **Background** | Embed CT in MDO doctrine; risk of neglect under peer focus. | Focus on training, exercises, civil–military/private ties. | CT must be both doctrinally embedded and practically exercised. |
| **CT Effectiveness** | Reactive, cyber key frontier, doctrinal gaps. | Exercises too conventional/reactive, lack foresight. | Shift to anticipatory posture across doctrine & training. |
| **MDO Integration** | Four pillars—unity, interconnectivity, creativity, agility. | Call for MDCT doctrine, foresight, OSINT, scenarios. | Doctrinal pillars should underpin training reforms. |
| **Capabilities** | Special forces, intelligence, non-military, psy-ops. | Training, OSINT, cyber/tech partnerships. | Strategic CT tools + practical training/partnerships. |
| **Cooperation** | Need trust-based intel, address underground dimension. | Structured civil–military/private sector partnerships. | Institutionalized cooperation combining both views. |
| **Legal/Political** | Legal anchors, sovereignty gaps, Allied divergence. | National laws restrict cooperation; seams exploited. | Need convergence to avoid fragmentation. |
| **Conclusions** | Institutionalize CT, integrate MDO, invest, converge. | Reform training, embed cooperation, legitimacy. | Unified CT-MDO = doctrinal + operational alignment. |

*Figure 7 Condensed Group 1 & Group 2 Synthesis*

# Findings and Recommendations

## Introduction

The workshop began with a scenario underscoring NATO's potential vulnerability to a multi-domain terrorist assault while focused on deterring state-based aggression. This scenario was not intended as fiction, but as a reminder that terrorism remains adaptive, transnational, and capable of exploiting blind spots across cyber, space, information, and societal domains.

Discussions reaffirmed what NATO's 2022 Strategic Concept and the Counter-Terrorism Policy Guidelines (2021) already recognize: counter-terrorism (CT) is an essential element of the Alliance's collective security, requiring both adaptation and cohesion. Terrorism, as highlighted in NATO's strategic documents, "in all its forms and manifestations, remains a persistent threat to our populations, international peace, and security."

The workshop concluded that CT in the multi-domain era is not peripheral but central to NATO's adaptability, credibility, and deterrence posture. Findings are clustered below into five thematic areas, followed by consolidated recommendations.

## NATO's Current Posture

The Counter-Terrorism Policy Guidelines have established a solid framework for prevention, protection, and response. They emphasize awareness, capabilities, engagement, and increasingly acknowledge the role of emerging technologies. Yet, the workshop identified persistent gaps:

- **Domain imbalance**: Current CT approaches remain oriented toward land, air, and maritime threats, while gaps persist in cyber, space, and cognitive domains.
- **Critical infrastructure**: Energy, telecommunications, transport, and cyber networks remain highly vulnerable to terrorist disruption.
- **Reactive posture**: NATO's CT posture remains largely demand-driven by nations, rather than proactive at the Alliance level.

This echoes NATO's resilience agenda and the Baseline Requirements for Civil Preparedness, but participants stressed the need for stronger multi-domain integration to ensure resilience against hybrid terrorist threats.

## Doctrinal and Strategic Adaptation

As NATO adapts its doctrine through the Concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA) and the War-Fighting Capstone Concept (NWCC), CT must also be doctrinally reframed. Discussions emphasized four qualities NATO must reinforce:

- **Unity**: Greater political cohesion and shared legal standards are essential. Divergent definitions of terrorism hinder effective action.
- **Interconnectivity**: Faster, broader, and more secure intelligence sharing with Allies, partners, industry, and civil society is crucial.
- **Creativity**: Innovative tools (AI-enabled analysis, counter-narratives, disinformation tracking) must be integrated into NATO's CT approach.
- **Agility**: Responses must be rapid, multi-domain by design, and flexible to ambiguous environments.

Group-1 underscored the risk of endless definitional debates, while Group-2 recommended a pragmatic approach: pushing for international legal standards to classify terrorist versus non-terrorist actors. Importantly, participants stressed that the cultural and human dimension of CT must not be neglected, in line with NATO's emphasis on human security and the Women, Peace, and Security (WPS) agenda.

**Embedding CT within Operational Art**

Counter-terrorism must be embedded within NATO's core tasks of deterrence and defence, crisis prevention and management, and cooperative security. Participants stressed that CT should not remain parallel or auxiliary, but integral to operational planning and execution.

Key points include:

- Aligning psychological and information operations with CT objectives to counter terrorist narratives.
- Ensuring political and legal clarity for action in cyber and space domains, as stressed in NATO's Cyber Defence Pledge.
- Recognizing terrorism as inherently hybrid—requiring synchronized use of diplomatic, informational, military, policing, and economic tools.
- Establishing specialized CT structures (e.g., Financial CT Office, Cyber CT Office), modelled on SCO-RATS or the EU's Horizon scanning system.

Stability policing and gendarmerie-type forces were highlighted as unique enablers within NATO's CT posture. Their dual military-police character allows them to:

- Bridge gaps between military operations and public security.
- Provide rapid law enforcement capacity in fragile, post-crisis, or high-threat environments.

- Support local policing institutions in restoring order and countering extremist influence.
- Enhance community engagement to contest radicalization, aligning with NATO's Human Security approach.

These constabulary-type forces embody NATO's doctrine of stability policing, already referenced in Allied Joint Doctrine (AJP-3.22), and should be more systematically integrated into CT–MDO operational concepts.

**Capabilities, Training, and Education**

Participants noted critical gaps in NATO's capabilities and training for multi-domain CT:

- **ISR and situational awareness**: NATO's ISR assets are underutilized for CT purposes.
- **Exercises**: Current scenarios do not adequately test multi-domain terrorist threats.
- **Training**: Need for cyber incident response, electronic warfare, OSINT, and cross-domain command skills.

Education and training must prepare future leaders to think multi-domain, fostering foresight and anticipation rather than reactive responses. Training frameworks should:

- Incorporate virtual/live-synthetic exercises and red-teaming.
- Systematically involve stability policing and gendarmerie-type forces to test hybrid CT responses.
- Strengthen interoperability between military, police, and civilian actors.

The private sector was also emphasized as an indispensable partner, particularly in cyber, satellite, telecommunications, and financial domains. This reflects NATO's Comprehensive Approach and the need for structured civil-military-private sector cooperation.

**Technology and Foresight**

The workshop confirmed the importance of NATO's Emerging and Disruptive Technologies (EDT) roadmap in shaping CT futures. Terrorists are likely to exploit AI, big data, drones, and quantum technologies for disinformation, swarming, and cyber disruption. NATO must turn these tools into advantages: predictive analytics, real-time monitoring, and strategic communications.

Foresight emerged as a critical multiplier. NATO should embed horizon scanning, scenario modelling, and contingency rehearsals into CT planning. This aligns with NATO's Innovation Fund and the Defence Innovation Accelerator for the North Atlantic (DIANA), which aim to prepare for multiple plausible futures and minimize the risk of strategic surprise.

**Consolidated Recommendations**

Based on discussions, five consolidated recommendations were formulated:

1. **Expand CT Guidelines**: Fully integrate cyber, information, underground, and policing domains; shift from reactive to proactive posture.
2. **Strengthen Unity and Standards**: Avoid definitional deadlocks; establish shared legal/strategic standards; align with NATO's CT Policy Guidelines and WPS commitments.
3. **Embed CT in Operational Art**: Create specialized CT structures; integrate stability policing and gendarmerie-type forces; ensure resilience of infrastructure and cognitive protection.
4. **Modernize Training and Partnerships**: Institutionalize multi-domain CT exercises; incorporate constabulary forces; strengthen OSINT-driven awareness and structured civil-military-private cooperation.
5. **Invest in Technology and Foresight**: Prioritize AI, unmanned systems, cyber defence, satellites, and foresight mechanisms in CT planning; leverage DIANA and NATO Innovation Fund resources.

**Concluding Assessment**

The scenario presented at the beginning highlighted NATO's potential unpreparedness for a multi-domain terrorist strike. Workshop discussions and findings demonstrate that such an outcome is not inevitable. By embedding foresight, adapting doctrine, strengthening stability policing, investing in capabilities and training, and consolidating partnerships, NATO can remain resilient and credible.

Counter-terrorism and multi-domain operations are no longer parallel tracks but converging realities. The real challenge for NATO is not whether to adapt, but how quickly and cohesively adaptation can occur, in alignment with the Strategic Concept 2022. Academics, practitioners, and NATO stakeholders share responsibility in translating these recommendations into concrete, actionable measures that will safeguard the Alliance against multi-domain terrorism.

| Thematic Area | Key Issues | Recommendations |
|---|---|---|
| **NATO's Current Posture** | Domain imbalance (land/air/maritime vs. cyber/space/cognitive);<br>Critical infrastructure vulnerabilities;<br>Reactive posture (nation-driven). | Expand CT Guidelines: integrate cyber, info, underground, policing;<br>Shift to proactive posture. |
| **Doctrinal & Strategic Adaptation** | Unity (political cohesion);<br>Interconnectivity (intelligence sharing);<br>Creativity (AI, counter-narratives);<br>Agility (rapid, multi-domain response). | Strengthen unity and legal/strategic standards;<br>Align with WPS and CT Policy Guidelines. |
| **Embedding CT in Operational Art** | CT must be integral to deterrence, defence, crisis management;<br>Hybrid threat response;<br>Stability policing and gendarmerie as enablers;<br>Need for specialized CT structures. | Embed CT into operational art;<br>Create specialized CT offices;<br>Integrate stability policing. |
| **Capabilities, Training & Education** | ISR underutilized;<br>Exercises don't test multi-domain terrorism;<br>Need for cyber/OSINT/cross-domain skills;<br>Civil-military-private cooperation essential. | Modernize training and exercises;<br>Strengthen OSINT-driven awareness;<br>Involve constabulary forces. |
| **Technology & Foresight** | Terrorists exploiting AI, drones, quantum;<br>NATO must use EDTs for predictive analytics, monitoring;<br>Foresight and horizon scanning critical for strategic surprise. | Invest in AI, cyber defence, unmanned systems, foresight;<br>Leverage DIANA and Innovation Fund. |

*Figure 8 Findings and Recommendations - Summary Table*

# Appendix

# Schedule

**Day 1: Strategic Alignment & Understanding the Challenge**

| Time | Session |
|---|---|
| **09:30–09:35** | Welcome & Opening Remarks<br>**Col. Halil Sıddık AYHAN,**<br>**COEDAT Director** |
| **09:35–09:40** | Remarks of Workshop Director<br>**LTC. Dietrich Klaus JENSCH** |
| **09:40-09:45** | Workshop Objectives and Desired Outcomes<br>**Assoc. Prof. Emrah ÖZDEMİR, Academic Adviser** |
| **09:45–10:05** | Keynote Address<br>**Mr. Gabriele CASCONE, NATO HQ** |
| **10:10–10:50** | Session 1: Strategic Foresight & Evolving Threats<br>**Mr. Oğuz KALAYCIOĞLU (VTC) NATO-ACT**<br>**Dr. Roderick PARKES NDC** |
| **10:50-11:10** | Coffee Break |
| **11:10-11:50** | Session 2: NATO's Current CT Approach<br>**LTC Claus SLEMBECK**<br>**Assoc. Prof. Özgür KÖRPE** |
| **11:55–12:35** | Session 3: CT and Future Warfare<br>**Professor Michael LISTER, UK**<br>**Dr. Ridvan Bari URCOSTA, NDC** |
| **12:35–13:45** | Lunch Break |
| **13:45–14:05** | Session 4: NATO's Concept for MDO and CT Approach<br>**Assoc Prof. Emrah ÖZDEMIR, NDU** |
| **14:10–14:50** | Session 5: CT Training in MDO Concept<br>**Dr. Zeynep SÜTALAN**<br>**Mr. Berke L. ÇAPLI** |
| **14:50–15:10** | Session 6: Workshop Aims & Group Formation |
| **15:10–15:30** | Coffee Break |
| **15:30–16:10** | Group Work Begins |

**Day 2: Group Work, Synthesis, and Recommendations with Academicians**

| Time | Session | Details |
|---|---|---|
| **09:15–11:00** | Group Work (Continued) | In-depth development of group topics. |
| **11:00–11:15** | Coffee Break | |
| **11:15–12:30** | Group Work Finalization | Prepare structured presentations. Identify priority recommendations. |
| **12:30–13:30** | Lunch Break | |
| **13:30–14:20** | Group Presentations | Group 1: Doctrinal Proposals (20 min + Q&A). Group 2: Training & Capability Proposals (20 min + Q&A). |
| **14:20–14:40** | Coffee Break | |
| **14:40–15:00** | Moderator's Synthesis of Key Takeaways | Cross-group integration. Draft policy and training outputs. |
| **15:00–15:30** | Plenary Discussion: Refining the Recommendations | Open-floor feedback session. Final agreement on workshop conclusions. |
| **15:30–15:45** | Next Steps & Final Remarks | Post-workshop deliverable timeline. Role of COEDAT in forwarding outputs to NATO HQ/ACT. Closing remarks. |

# List of Speakers

| S.N. | Name Surname | Institution | Presentation Subject |
|---|---|---|---|
| **1** | Mr. Gabriele Cascone | Head of Counter-Terrorism Section, Emerging Security Challenges Division, NATO | Keynote Speech |
| **2*** | Mr. Oğuz Kalaycıoğlu | Senior Enterprise Architect NATO ACT | Foresight Analysis |
| **3** | Dr. Roderick Parkes | Researcher, NATO Defence College | Current Threat Environment |
| **4** | LTC Claus Slembeck | NATO ACT CT SME | CT in NATO Approach |
| **5** | Professor Michael Lister | Oxford Brooks University | Contemporary CT Approaches from Critical Perspective |
| **6** | Assoc. Prof. Özgür Körpe | Turkish NDU War College | Future of Warfare and CT |
| **7** | Dr. Ridvan Bari Urcosta | Fellow of NATO Defence College | Future Warfare |
| **8** | Assoc. Prof. Emrah Özdemir | Turkish NDU Military Academy | CT in MDO Context |
| **9** | Dr. Zeynep Sütalan | CoE DAT | MDO and CT Training |
| **10** | Mr. Berke L. Çaplı | NATO STO, SAS Leader | War Gamin in CT Training |

***Presentation will be through VTC.**

# List of Participants for Group Discussions

| S.N. | Rank/Title | Name Surname | Institution | Discussion Group |
|---|---|---|---|---|
| **Group 1: Strategic and Doctrinal Adaptation** | | | | |
| 1 | Head of Division | Gabriele Cascone | NATO HQ | Practice |
| 2 | Col. Assoc. Prof. | Mehmet Kurum | Gendarmerie and Cost Guard Academy | Practice |
| 3 | (R) Col. Assoc. Prof. | Özgür Körpe | National Defence University (Visiting) | Practice |
| 4 | Col. Dr. | Bürke Uğur Başarenel | Gendarmerie and Cost Guard Academy | Practice |
| 5 | (R) Col. Assoc. Prof. | Haluk Karadağ | Başkent University | Practice |
| 6 | Dr. | Tarık Solmaz | Lecturer | Practice |
| 7 | LTC. | Claus Slembeck | NATO ACT CT SME | Practice |
| **Group 2: Capability and Training Development** | | | | |
| 1 | Dr. | Zeynep Sütalan | CoE DAT | Training |
| 2 | Prof. | Michael Lister | Oxford Brooks University | Training |
| 3 | Dr. | Merve Önenli Güven | National İntelligence Academy | Training |
| 4 | Assoc. Prof. | Serkan Yenal | National Defence University | Training |
| 5 | Dr. | Ridvan Bari Urcosta | Warsaw University/NATO Defence College | Training |
| 7 | Dr. | Roderick Parkes | NDC | Training |

# Biographies of Presenters


**Col.Halil Sıddık Ayhan**

COEDAT Director

Colonel AYHAN, appointed Director of the NATO Centre of Excellence Defence Against Terrorism on 16 August 2024, graduated from the Turkish Military Academy in 1998. Over his career, he has served in a wide range of tactical, operational, and strategic roles within the Turkish Armed Forces, including Platoon and Company Commander, staff positions in logistics, operations, and training, as well as senior appointments such as Regiment Commander, and Chief of Operations at the Operational Headquarters. His multinational experience includes service in Bosnia-Herzegovina (2010), Kosovo (2016), and as Operations, Defence, and Capability Officer at the Turkish Military Representative Delegation to NATO (2018–2021). A graduate of the War College Staff Officer Course, he also holds a master's degree in international Affairs from Bilkent University (2003).

**LTC. Dietrich JENSCH**

Workshop Director

Dietrich Klaus Jensch, a German Army officer, currently serves as Senior National Representative and Branch Chief, Concept and Policy (since September 2024). From 2020 to 2024, he was Germany's Defence Attaché in Serbia following his participation in the Serbian General Staff Course, and earlier, he directed the German military attaché training course (2017–2019). He previously served as German Defence Attaché in Lebanon (2014–2017) and held a series of command and staff assignments within Army Air Defence, ranging from platoon leader to battalion commander, as well as positions as a planning officer in the DEU/NL Corps, instructor at the Army Officers' School, and Aide-de-camp in an armoured division. His experience also includes public affairs roles, notably as spokesperson for Bundeswehr missions and operations at the Ministry of Defence in Berlin. He has operational experience from missions in the Balkans, Africa, and Asia, and holds a Master's degree in Pedagogics from the University of the German Armed Forces in Hamburg.

**Assoc. Prof. Emrah Özdemir**

Turkish Military Academy

He graduated from the Turkish Military Academy and served in various positions within the Gendarmerie General Command until 2018, when he voluntarily retired. He holds master's degrees in International Security and Terrorism and Political Science and completed his Ph.D. at Swansea University (UK) with a dissertation on counterinsurgency in Afghanistan. Since 2022, he has been teaching at the National Defence University, with visiting scholar experience at the NATO Defence College (Rome) and the NATO Stability Policing Centre of Excellence (Vicenza). He currently lectures on intelligence, security, political violence, war, and strategy at undergraduate and graduate levels at the National Defence University and the Gendarmerie and Coast Guard Academy.

**Gabriele Cascone**

Head of the Counter-terrorism Section Emerging Security Challenges Division, NATO

Gabriele Cascone spent the first part of his career as an officer in the Carabinieri Corps and then joined the NATO International Staff, where he still works as head of the Counter-terrorism section in the Emerging Security Challenges Division. The focus of his career at NATO has been mostly on the Western Balkans and on the security situation in the Middle East and North Africa region.

**Oğuz Kalaycıoğlu**

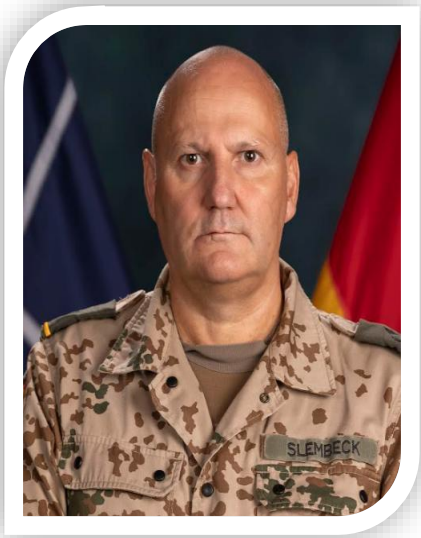
Senior Enterprise Architect · NATO Allied Command Transformation (ACT)

With over 30 years of experience in the defence sector, Oğuz Kalaycıoğlu specializes in large-scale system design and has contributed to numerous defence, security, safety, and NATO projects. Currently, he manages and consults on projects focused on information and communication technologies, interoperability, digital transformation, modernization, and research & development.

**Dr. Roderick Parkes**

Researcher NATO Defence College

Dr. Parkes has worked for national and international think tanks across Europe over the past two decades. The focus of his research has been non-state threats and hybrid warfare, the management of international flows and the protection of critical infrastructure, crisis response and the geopolitical drivers behind internal security threats. He has managed research projects and has extensively applied methodologies of strategic foresight. Before joining the NATO Defence College, he was the deputy director of the German Council on Foreign Relations (DGAP) in Berlin and led its Alfred von Oppenheim Centre on the Future of Europe.




**LTC. Claus Slembeck**

SME at HQ ACT NATO

He is currently serving as NATO SACT SPP PLP Subject Matter Expert for CT and CHT. A graduate of the University of the Federal Armed Forces in Hamburg, Germany, with an M.A. in History and Politics, he has held key intelligence and policy positions including Section Head for INTEL Plans & Policy at NATO JFC Lisbon, Section Head IRM/CM at NATO MNC NE in Szczecin, and Chief of Staff of the All Source Information Fusion Cell (ASIFU) in MINUSMA, Mali (2015–2016). His distinguished career also includes service as Deputy Defence Attaché and Army Attaché at the German Embassy in Beijing, as well as senior roles within the German Army HQ in Strausberg at the Land Intel Centre and the G2 Plans & Policy Section. He has operational experience from multiple missions including SFOR (2000–2001), ISAF (2002), KFOR (2006), and MINUSMA (2015–2016).

**Assoc. Prof. Özgür Körpe**

Visiting Scholar at NDU

He graduated from the Turkish Military Academy and served in various positions within the Turkish Armed Forces. He holds master's degrees in National and International Security Strategies and in Defence and Security Management, as well as a Ph.D. in Political Science and International Relations. He also completed the Command and Staff Training at the Army War College and the Joint Command and Staff Training at the Joint War Institute. Dr. Körpe previously served as faculty member at the Army War College and later taught at Istanbul Aydın University (2020–2022). He continues to lecture at the National Defence University and across various institutions on security, defence, and international relations.

**Prof. Michael Lister**

Oxford Brookes University, UK.

His research focuses on the intersections between citizenship and terrorism/counter-terrorism. He is the author of Public Opinion and Counter-terrorism: Security and Politics in the UK (2023) and co-editor of The State: Theories and Issues 2nd Edition (2022). He has published research in Political Studies, Parliamentary Affairs, International Relations, and The British Journal of Politics amongst others. He has presented his research findings widely, including to the UK Home Office, the Welsh Assembly and UK police officers

**Dr. Ridvan Bari Urcosta**

Fellow at NATO Defence College

He is a lecturer at the University of Warsaw's Department of Strategic Studies and International Security, where he earned his Ph.D. in Security Studies. He teaches courses titled Russia from the Middle East to the Global South, as well as Future Warfare, European Institutions, and International Military Relations. In addition to his academic role, Dr Urcosta is an analyst at Geopolitical Futures (formerly Stratfor), a U.S.-based think tank, where he specializes in the Eurasia region. He also worked for the Polish think tank Strategy and Future for four years. Dr Urcosta was born in Abkhazia, Georgia.

**Dr. Zeynep Sütalan**

Independent Researcher

Dr. Zeynep Sütalan holds a PhD in International Relations from the Middle East Technical University. From 2005 to 2011, she served as a concept specialist at the Centre of Excellence Defence Against Terrorism (COE-DAT). She has delivered lectures on terrorism at COE-DAT and at the Partnership for Peace Training Centre in Ankara. Her research interests include terrorism, counterterrorism, gender and terrorism, as well as the history, politics, and economics of the Middle East. Between 2018 and 2022, she was an adjunct lecturer in the Department of International Relations at Atılım University. From 2019 to 2023, she served as the academic advisor for COE-DAT's Workshop Series on Gender in Terrorism and Counterterrorism. Dr. Sütalan continues to collaborate closely with COE-DAT, contributing through lectures, research projects, and education and training activities.

**L. Berke Çaplı, MSc.**

Chair at NATO STO, Multi-Domain Wargaming Research Task Group

He is a PhD candidate at the University of Edinburgh, specializing in the intersection of social trauma and authoritarianism. He brings over seven years of experience in urban technology as co-founder of Placemaking AI, a company that applies location intelligence to automate commercial real estate operations. For more than a decade, he has chaired international research groups on wargaming, defence, security, and strategic decision-making, and at 25 became the youngest chair of a NATO Science and Technology Organization research group, leading pioneering studies on artificial intelligence, behavioural analysis, and multi-domain operations. Beyond academia and defence research, he co-founded KızBaşına, one of Türkiye's largest women's rights organizations, where he has been a strong advocate for gender equality and policy reform.

CENTRE OF EXCELLENCE
DEFENCE
AGAINST TERRORISM
ANKARA - TURKEY
COE-DAT

**Acknowledgement**

**Assoc. Prof. Emrah ÖZDEMİR**

*Academic Adviser and Editor*

**LTC. Dietrich Klaus JENSCH**

*Workshop Director*

**Ms. Müge MEMİŞOĞLU AKAR**

*Workshop Co-Director*

**Ms. Elif Merve DUMANKAYA**

*Rapporteur*

**Ms. Derya DEĞER ÇEKİÇ**

*Rapporteur*

**Contributors**

**Col. Dr. Bürke Uğur BAŞARANEL**
**LTC. Claus SLEMBECK**
**Mr. Gabriele CASCONE**
**Capt. (N) Hakan GÖMENGİL**
**Col. (R) Assoc. Prof. Haluk KARADAĞ**
**Mr. L. Berke ÇAPLI**
**Mr. Oğuz KALAYCIOĞLU**
**Col. Assoc. Prof. Mehmet KURUM**
**Dr. Merve ÖNENLİ GÜVEN**
**Prof. Michael LISTER**
**Col. (R) Assoc. Prof. Özgür KÖRPE**
**Dr. Ridvan Bari URCOSTA**
**Dr. Roderick PARKES**
**Assoc. Prof. Serkan YENAL**
**Dr. Tarık SOLMAZ**
**Dr. Zeynep SÜTALAN**

**Col. Halil Sıddık AYHAN (TÜR A)**

***Director, COE DAT***

**Address: Devlet Mahallesi İnönü Bulvarı Süleyman Emin Caddesi No:65 Çankaya 06582 Ankara, Türkiye**
**P.O. Box: P.K.- 57 06582 Bakanlıklar-Ankara, Türkiye Phone: +90 312 425 82 15 Fax: +90 312 425 64 89 E-mail: info@coedat.nato.int**