YOU ARE IN THE C-IED

CHESSBOARD

INSIGHTS FROM NATO's C-IED EXPERTS

JUN 2026 | ISSUE 05

NATO OTAN
Accredited COE

EDITORIAL STAFF

Director
COL Javier Sanz Maldonado (ESP A)

Executive Director
COL Christopher Bartos (USA A)

Editorial Production
LTC Carlos García de Paredes Ucero (ESP MC)
1st LT (Reservist) Víctor Sánchez del Real (ESP A)

Layout & Graphics
SGT Diego Ropero Pastor (ESP A)

Language Assistant
Sara Infantozzi Hurtado (ESP CIV)

Contributors
AtN Branch
PtF Branch
DtD Branch

Authors

LTC José Manuel Rufas Simón (ESP A)
LTC Matthias Döpping (DEU A)
LTC Carlos García de Paredes Ucero (ESP MC)
LTC Félix Ortega Medina (ESP A)
LTC José Manuel Veiga Torres (ESP A)
LTC Robert Tranberg (SWE A)
Lt Cdr Murat Aydogmus (TUR N)
MAJ Juan Manuel Mancilla López (ESP MC)
MAJ Alberto Brunhöfer García (ESP A)
MAJ Georgios Krikelis (GRC A)
MSGT David Herráiz López (ESP A)

DISCLAIMER

CONTENTS

Counter-Improvised Explosive Devices Centre of Excellence

NATO Accredited Centre of Excellence

Ctra. M-618 Colmenar Viejo-Torrelodones km. 14
28240 hoyo de manzanares, madrid-spain
+34 91 856 10 48
info@ciedcoe.org
www.ciedcoe.org

NEWS FROM OUR WATCH

C-IED COE
Director's Letter

Dear C-IED Community of Interest,

This edition of the Chessboard reflects the continued evolution of the Counter-IED fight in an increasingly complex and multi-domain security environment. As the threat adapts, leveraging emerging technologies, hybrid networks and new delivery vectors will foster our collective understanding, preparedness and response to these challenging risks.

In this issue, we highlight selected contributions that capture this transformation. Articles explore the integration of C-IED within NATO's Warfare Development Agenda, the growing relevance of lessons learned from recent conflicts, including the use of unmanned systems as IED vectors. We also present insights into training and education initiatives, technological innovation and the importance of interagency and multinational cooperation in addressing the full spectrum of the IED threat.

This magazine continues to serve as a platform for the C-IED Community of Interest, connecting practitioners, planners and decision-makers, and reinforcing the exchange of knowledge that underpins operational effectiveness. As highlighted in recent analyses, the C-IED approach must be fully integrated across planning and execution processes, combining the pillars of Attack the Networks, Defeat the Device and Prepare the Force into a coherent and strategic framework.

We are pleased to announce that this edition of the Chessboard will be formally distributed during the C-IED COE Annual Conference 2026 (CIEDAC 26) in Valencia, providing an opportunity to engage directly with the community, share perspectives and strengthen collaboration among Allies, Partners and stakeholders.

As we move forward, our collective effort remains focused on anticipating the threat, adapting our capabilities and ensuring that C-IED remains a relevant and effective contributor to NATO's deterrence and defence posture.

With warm regards,

Javier Sanz Maldonado
Colonel, Spanish Army
Director, C-IED Centre of Excellence

C-IED COE HIGHLIGHTS

NATO's Defence Against Terrorism Programme of Work (DAT POW) support to C-IED

As terrorist methods evolve, and as state and non-state actors increasingly blend conventional force with asymmetric tactics, NATO's ability to anticipate and disrupt such threats hinges on a complex - but often overlooked - pillar of its defence architecture: the Defence Against Terrorism Programme of Work (DAT POW).

While seldom in the spotlight, the Programme constitutes one of the Alliance's most enduring engines of innovation, driving forward the development of capabilities that protect troops, populations and critical infrastructure from a wide spectrum of terrorist threats.

Created in 2004 and continually adapted since, DAT POW supports NATO's broader counter-terrorism strategy across three principal pillars: awareness, capabilities and engagement. In practice, this means the Programme sustains a multinational ecosystem of exercises, trials, concept-development activities, standardization work and research initiatives.

Its primary aim is to address the terrorist use of IEDs, drones, CBRN agents, cyber-enabled tools and other disruptive technologies. What makes DAT POW particularly powerful is its flexibility: its activities align quickly with emerging trends, whether it is the rise of weaponized uncrewed systems, the exploitation of artificial intelligence by violent extremist organizations, or the changing C-IED landscape in theatres like the Middle East, Sahel or Eastern Europe.

A significant share of DAT POW's work is channeled through NATO's accredited Centres of Excellence (COEs), amongst which we can mention the Counter-Improvised Explosive Devices (C-IED) COE, the Explosive Ordnance Disposal (EOD) COE, the Joint Chemical, Biological, Radiological and Nuclear Defence (JCBRN) COE and the Defence Against Terrorism (DAT) COE.

These institutions deliver the specialised knowledge, interoperability testing and doctrinal development that underpin NATO's operational edge. Recent efforts include multinational EOD trials, live testing of Counter-Unmanned Aerial Systems (C-UAS), high-fidelity harbour and route-clearance exercises, and the development of AI-enabled detection tools.

Education and training remain equally central: the DAT COE alone is running a robust programme of residential and mobile courses, from counter-terrorism doctrine and "Terrorist Use of Weapons of Mass Destruction" modules, to workshops on Special Operation Forces' roles in crisis response, and the impact of climate change on terrorism.

Academic research tied to DAT POW has expanded as well, with studies on the Russia-Ukraine war's effect on terrorism, and the weaponization of artificial intelligence, shaping strategic understanding across the Alliance.

Yet the significance of DAT POW extends beyond its visible activities. It also acts as a bridge between nations, intelligence organizations, academia and indus-

try, enabling NATO to access emerging technologies and to test them in conditions approaching the real operational environment.

Through the Programme, the Alliance evaluates prototypes, validates new operational concepts, and identifies the technological gaps that must be filled to stay ahead of adversaries. This dynamic ecosystem fosters interoperability - between nations, between services and between military and civilian institutions - ensuring that lessons learned are rapidly translated into doctrine and shared across the Alliance.

Despite its impact, certain aspects of the Programme remain deliberately opaque. NATO does not disclose consolidated budget figures or detailed project roadmaps for DAT POW, primarily due to security considerations and the sensitive nature of many of the technologies involved. The absence of publicly available financial data is understandable: projects linked to IED neutralization, C-UAS defeat systems, CBRN detection, technical exploitation or intelligence support demand strict protection. Moreover, the Programme's adaptive nature means that initiatives can be launched or modified quickly as threat patterns evolve.

For Centres like the C-IED COE, the DAT POW is indispensable. It not only provides a structured framework for capability development, but also connects the Centre's expertise with NATO decision-makers and operational planners. Crucially, DAT POW also funds selected C-IED COE events and courses, enabling the Centre to expand its impact and reach.

This includes flagship initiatives such as CIEDAC25 in Málaga, which benefited from DAT POW support and stands as a prime example of how the Programme amplifies multinational training, knowledge-sharing and innovation. Whether through financial support to exercises such as Northern Challenge, the integration of C-IED considerations into major NATO events, or participation in research, trials and experimentation,

DAT POW significantly enhances the Centre's influence and operational relevance across the Alliance. Within the broad scope of the DAT POW, the C-IED COE plays a central role as NATO's primary hub for Counter-IED expertise. Its contributions extend from doctrine and concept development to technical analysis, training and operational support, ensuring that the Alliance maintains a coherent and modern approach to countering IED threats across all domains.

Through systematic participation in DAT POW activities, the Centre provides threat assessments, supports capability development and offers unique insights into emerging tactics, techniques and technologies used by state and non-state actors. Its periodic analytical reports and specialized expertise feed directly into NATO's collective awareness and help shape capability priorities for Counter-IED operations.

The Centre's operational value is equally visible in its support to DAT POW-linked exercises, trials and experimentation events. Whether integrating C-IED objectives into NATO-level exercises, contributing technical-exploitation expertise to field activities, or supporting multinational demonstrations of new detection and neutralization technologies, the C-IED COE ensures that counter-IED considerations remain firmly embedded in NATO's training and readiness architecture.

Its positions on Technical Exploitation and Battlefield Evidence, areas increasingly critical for attribution, intelligence and legal processes, make the Centre even more relevant as the Alliance adapts to hybrid and Multi-Domain environments.

Ultimately, the integration of the C-IED COE within the DAT POW strengthens both the Centre and the Alliance. By aligning its projects, education initiatives and analytical outputs with the Programme's priorities, the Centre amplifies its influence, contributes directly to NATO's strategic transformation efforts, and reinforces its role as the definitive multinational reference point for Counter-IED knowledge and capability development.

2026 Budget Allocation

The DAT POW for 2026 allocates its budget to a diverse portfolio of capability-development initiatives supporting NATO's evolving defence and security priorities. The investments reinforce NATO's commitment

to counter-terrorism, counter-IED, counter-UAS, biometrics, underwater protection, engineering, HUMINT innovation, training technologies and the adoption of emerging disruptive technologies.

The POW reflects the increasing complexity of the strategic environment, highlighting urgent needs in Multi-Domain Operations, critical infrastructure protection, rapid innovation and integration of AI-enabled tools across Alliance forces.

Priority Funding Areas

1. Counter-Unmanned Systems (C-UxS): The largest funding block supports the rapid adoption of Counter-UAS and Counter-UxV capabilities, including interoperability trials (TIE26), naval C-UxV exercises, electronic countermeasures testing and UAV operator qualification initiatives. These projects directly reinforce NATO's response to the explosive proliferation of unmanned threats in modern conflicts.

2. Biometrics & Identity Intelligence: Investments include the NBTI workshop, Northern Spirit 26 biometrics exercise, and AI-enabled identity analysis tools. Strengthening biometric exploitation is a critical enabler for both counter-terrorism and AtN operations.

3. Underwater & Maritime Protection: A substantial portion funds capability development for the protection of Critical Undersea Infrastructure (CUI), including SOF-led experiments (BOLD MACHINA), VR-based situational awareness tools and unmanned maritime defence systems (MANTA II).

4. CBRN Defence & Medical Training: Live-agent CBRN training and an AI-supported VR lifesaver system ensure readiness against chemical and biological risks.

5. HUMINT & AI Innovation: Development of an AI companion to support HUMINT operators during live engagements.

6. Military Engineering & Force Protection: Funding for a software tool enabling standardized, high-fidelity vulnerability assessments across NATO.

7. EOD VR/XR Training: XR-based EOD training environments expand NATO's ability to train safely and realistically.

The 2026 DAT POW demonstrates NATO's strong emphasis on the capabilities of emerging and disruptive technologies, interoperability and agile adoption cycles, aligning closely with ACT's Rapid Adoption Action Plan (RAAP) and emerging requirements from the Warfare Development Agenda (WDA).

For the C-IED COE, the POW reaffirms its central role in NATO's capability development ecosystem, particularly in Attack the Networks, Technical Exploitation, and the integration of C-IED approaches into Multi-Domain and hybrid threat environments.

C-IED COE hosts successful NATO ACT Periodic Assessment visit

The Counter-Improvised Explosive Devices Centre of Excellence (C-IED COE) has successfully concluded a three-day Periodic Assessment visit conducted by a delegation from Allied Command Transformation (ACT), reinforcing its continued relevance and contribution to the Alliance.

The visit, held at the Centre's facilities in Hoyo de Manzanares, brought together subject matter experts and leadership from both organizations to conduct a comprehensive review of the Centre's activities, outputs and alignment with NATO accreditation criteria. The Periodic Assessment is conducted every three years to evaluate Centres of Excellence against established standards and to ensure their effectiveness in supporting NATO's transformation and operational requirements.

Throughout the visit, the C-IED COE demonstrated its integrated and multidisciplinary approach to countering improvised explosive device threats, encompassing the full spectrum of activities across Attack the Networks, Defeat the Device and Prepare the Force. Particular emphasis was placed on the Centre's contributions to doctrine development, education and training, operational support, and innovation in response to emerging and hybrid threats.

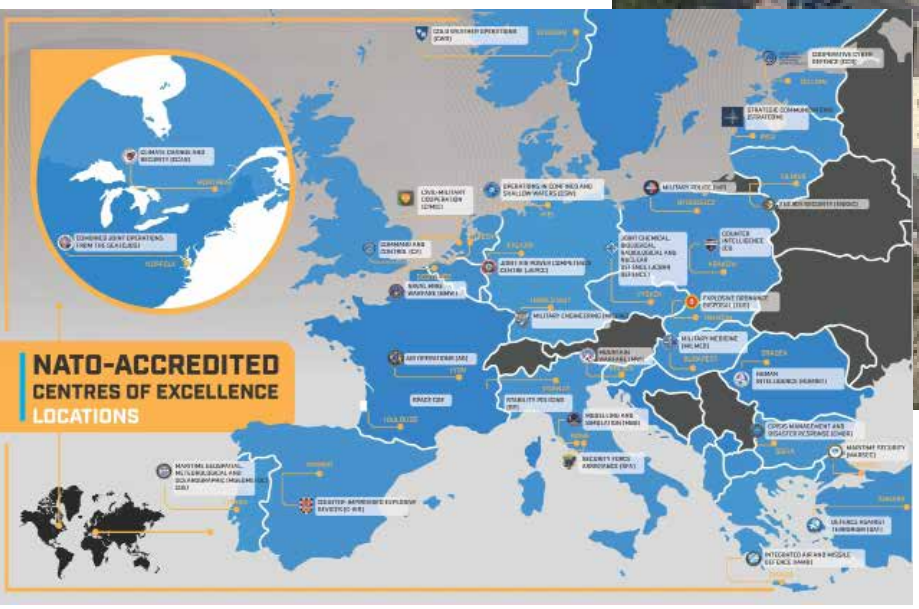
The first day of the assessment included a comprehensive briefing outlining the Centre's workforce, key activities and progress made since the previous assessment. The subsequent sessions focused on a detailed, collaborative review of the Periodic Assessment Questionnaire, conducted jointly by the C-IED COE staff and the ACT assessment team. This process enabled a transparent and constructive exchange, ensuring that the Centre's outputs and impact were accurately reflected.

The final day included staff engagements and informal interviews, providing additional insight into the Centre's expertise and internal processes. The visit concluded with a virtual debrief conducted with Major General Soto at Headquarters Allied Command Transformation in Norfolk, during which the assessment team presented their preliminary findings.

During the debrief, the ACT team highlighted the high level of professionalism, commitment and output demonstrated by the C-IED COE and indicated its intention to submit a favourable report as part of the Periodic Assessment process.

This successful evaluation underscores the C-IED COE's role as a key enabler within NATO's Warfare Development ecosystem, contributing to the Alliance's ability to anticipate, understand and counter evolving IED threats in a complex and multi-domain environment.

The C-IED COE remains committed to supporting NATO, its Allies and Partners through expertise, innovation and cooperation, ensuring that the Alliance maintains its operational effectiveness against one of the most persistent and adaptive threats in modern conflict.



WHAT IS A CENTRE OF EXCELLENCE?

A Centre of Excellence (COE) is an international military organization

COEs train and educate leaders and specialists from NATO member and partner countries. They assist in doctrine development, identify lessons learned, improve interoperability and capabilities, and test and validate concepts through experimentation. They offer recognised expertise and experience that is of benefit to the Alliance, and support the transformation of NATO, while avoiding the duplication of assets, resources and capabilities already present within the Alliance.

Role of the Centres of Excellence

COEs generally specialize in one functional area and act as subject-matter experts in their field. They distribute their in-depth knowledge through four pillars:

- Education, training, exercise and evaluation (ETEE)
- Analysis and lessons learned (A &LL)
- Doctrine development and standardization (DDS)
- Concept development and experimentation (CDE)

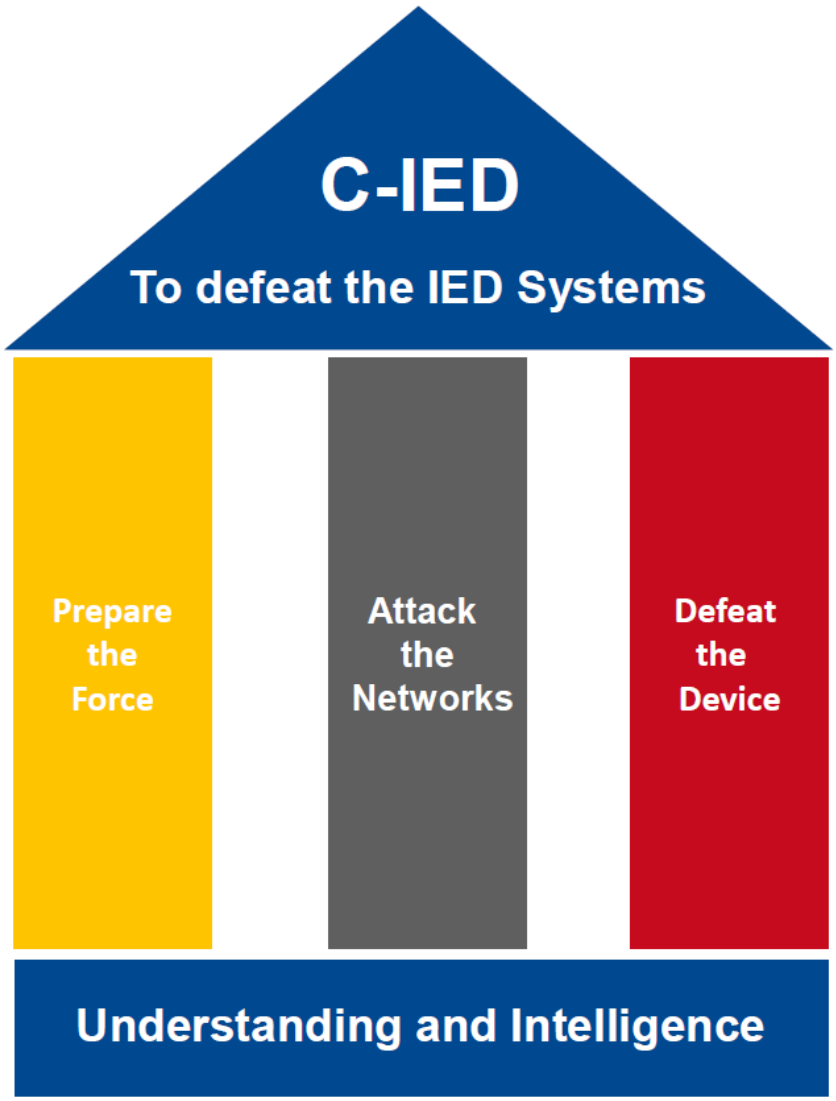
MORE INFO
act.nato.int/about/centres-of-excellence

COEs work alongside the Alliance even though NATO does not directly fund them and they are not part of the NATO Command Structure. They are nationally or multi-nationally funded and are part of a supporting network, encouraging internal and external information exchange to the benefit of the Alliance. The overall responsibility for the coordination and utilisation of the COEs within NATO lies with Allied Command Transformation (ACT), in coordination with the Supreme Allied Commander Europe (SACEUR).

Currently, there are 30 COEs with NATO accreditation. The working language of the COEs is generally English.

The C-IED COE is a proud member of the COE community

MISSION: to provide subject matter expertise in order to support the Alliance, its Partners and the International Community in the fight against IED system and to cooperate to increase security of Allied Nations and troops deployed in theatres of operations, reducing or eliminating the threats from improvised explosive devices used or for use, in particular by terrorist or insurgents.



FEATURED ARTICLES

Update on Maritime Explosive Threats in the Hormuz Strait

After the surprise attack by Israel and the United States of America over Iran on 28 February 2026, the risk of an Iranian closure of the Hormuz Strait is growing.

In fact, the area of the Arabian Gulf and the Hormuz Strait is not under the responsibility of the Iranian Navy, but the Iranian Revolutionary Guard Corps (IRGC) Navy forces.

Figure 1 – Allocation of IRGC Navy means along the way to the Hormuz Strait (Source: ALMA Research & Education Center)

The relatively narrow Hormuz Strait allows not only the use of ground-based anti-ship missiles, but also barreled artillery and loitering munitions launched from land.

In addition to bigger frigates and missile launcher vessels, IRGC Navy counts on several types of fast patrol boats (TONDAR Class, AZARAKHSH Class) able to carry anti-ship missiles, as well as fast attack boats (ASHURA Class, ZULFIKAR Class, TAREQ Class, SIRAJ Class, MIL-40 Class, RIB Class, TIR-II Class...) capable of using rockets, anti-ship missiles, anti-aircraft missiles, torpedoes and sea mines. Other smaller boats could also launch rockets and emplace sea mines.

Hard-to-detect small submarines, such as the GHADIR Class, provide the IRGC Navy with a covert strike capability through the employment of cruise missiles, torpedoes, anti-ship missiles and naval mines. Complementing these platforms, underwater Swimmer Delivery Vehicles (SDVs), including the AL-SABEHAT and E-GHAVASI models, enhance Iran's ability to conduct clandestine maritime infiltration, mine warfare and asymmetric naval operations in the confined waters of the Hormuz Strait

Apart from the wide MAHAM family of sea mines, Iran has received Chinese models like the EM52, a seabed-emplaced rising sea mine with a rocket-propelled explosive charge and an operating depth of at least 650 feet.

Iran has shown a weapon labeled "مین دریایی رونده" (moving sea mine) as well as the NAZIR-5 and AZHDAR explosive-laden unmanned underwater systems (UUVs).

Figure 2 – NAZIR-5 unmanned underwater vehicle (Source: www.defencesecurityasia.com/X)

Figure 3 –Iranian AZHDAR UUVs (Source: X)

Along with those UUVs used as a sort of maritime loitering munitions, IRGC Navy is also counting on explosive-laden unmanned surface vehicles (USVs).

In addition to the waterborne means, the unmanned aircraft systems (UASs) from Iran are capable of attacking: control rooms, armament, boarded helicopters, communications, sensors, radars and the electromagnetic warfare means of the vessels crossing the Hormuz Strait. The boarded or ground-based ARASH-2 model, the SHAHED series and the ABABIL series are good examples of long-range and payload explosive-laden UAS.

Even the newest loitering munitions, such as the Rezvan (GLMD-24W4.5-R2) model, could pose a threat to the vessels and forces along the Hormuz Strait, due to its range of 20 Km with a 25 Kg high-explosive antitank (HEAT) warhead.

Figure 4 – Iranian REZVAN loitering munition (Source: www.armyrecognition.com)

REZVAN is designed for direct battlefield use rather than long-range attack, capable of detecting, tracking and striking targets within a 20-km radius in a single mission cycle.

However, the proliferation of inexpensive autonomous systems introduces a distributed threat environment that cannot easily be neutralized through traditional fleet engagements. Instead of confronting large warships directly, unmanned underwater drones can exploit stealth, endurance and numerical advantage to impose operational costs on superior naval forces.

The strategic calculus therefore shifts toward defending against numerous small threats rather than confronting a small number of high-value adversary platforms. In environments like the Strait of Hormuz, this dynamic may favor asymmetric actors capable of deploying large numbers of low-cost underwater drones. Such systems do not require extensive naval infrastructure or highly trained crews, allowing them to be deployed rapidly and at scale.

REFERENCES

- X (former TWITTER)
- www.hisutton.com
- ALMA Research and Education Center
- www.defencesecurityasia.com

Recent technological advances in underwater maritime protection

1. Introduction

The underwater domain has become an increasingly critical component of maritime security, driven by the growing reliance on ports, offshore infrastructure, subsea energy systems and naval operations. As maritime activity expands, so does the diversity and sophistication of underwater threats. These threats range from conventional mines and improvised devices to stealth intrusions by divers or unmanned systems, all of which pose significant risks to both military and civilian assets.

Detecting such threats is inherently challenging due to the complex and dynamic nature of underwater environments. Factors such as limited visibility, signal attenuation and environmental variability significantly constrain sensing capabilities. For this reason, modern detection strategies focus primarily on identifying physical objects and anomalies such as unusual shapes, seabed disturbances or motion patterns, rather than directly detecting explosive materials.

In recent years, significant technological advances have transformed underwater maritime protection. The integration of artificial intelligence, autonomous systems, advanced sonar technologies and distributed sensing architecture has enabled more accurate, efficient and scalable detection and response mechanisms. This article provides a structured overview of these developments, highlighting how traditional methods are being enhanced by modern innovations.

2. Foundations of underwater threat detection

2.1 Sonar-based detection principles

Underwater detection has traditionally relied on acoustic sensing, as electromagnetic waves are rapidly attenuated in water. Sonar systems remain the primary technology for detecting and imaging underwater objects. By emitting sound waves and analyzing their reflections, sonar systems provide insight into the structure of the seabed and the presence of objects. Among the most widely used sonar technologies are Side-Scan Sonar (SSS) and Synthetic Aperture Sonar (SAS). SSS enables efficient wide area scanning and is particularly effective at identifying objects based on acoustic shadows and intensity variations. In contrast, SAS enhances resolution by combining multiple acoustic measurements, allowing for the detection of smaller or partially buried objects with greater clarity.

These systems can detect both metallic and non-metallic objects by identifying deviations in seabed texture, geometry and reflectivity. However, despite their technical capabilities, sonar-based detection has traditionally relied on manual interpretation. Operators must visually analyze sonar imagery, making the process time-consuming and dependent on experience, which can lead to inconsistencies in detection performance.

2.2 Environmental and operational challenges

The underwater environment presents several inherent challenges that complicate detection processes. Acoustic noise, seabed clutter and varying terrain conditions can obscure signals and increase false alarm rates. Additionally, water turbidity and light attenuation limit the effectiveness of optical sensors, particularly in deep or coastal waters.

A key difficulty lies in distinguishing between hazardous objects and benign seabed features, such as rocks, debris or man-made structures. Many objects share similar acoustic signatures, making reliable classification a complex task. These challenges highlight the limitations of traditional approaches and underscore the need for more advanced, automated and adaptive detection systems.

3. Technological advances in underwater maritime protection

3.1 Artificial Intelligence and data-driven detection

Artificial intelligence has emerged as a transformative technology in underwater detection. By enabling automated analysis of sonar and optical data, AI reduces reliance on human interpretation and improves both speed and consistency.

Deep learning models, particularly convolutional neural networks (CNNs), can extract complex features from high-dimensional data. These models can detect subtle patterns and anomalies that may not be easily recognizable by human operators. As a result, AI-based systems significantly improve detection accuracy while reducing false alarms.

The performance of these systems is closely tied to data quality. Preprocessing techniques such as denoising, contrast enhancement and super-resolution are critical for improving input data and ensuring that relevant features are preserved. Furthermore, diverse and representative datasets enable models to generalize across different environmental conditions and object types.

3.2 Object classification and predictive capabilities

Beyond detection, AI plays a crucial role in object classification, which is essential for distinguishing threats from non-threatening objects. Machine learning algorithms including support vector machines, ensemble methods and neural networks have demonstrated high accuracy in classifying sonar data.

In addition to classification, modern systems incorporate predictive capabilities. By analyzing motion patterns and historical data, AI models can estimate the future positions of detected objects. This is particularly important in dynamic environments where targets may move or where tracking continuity is required.

Such predictive analysis enhances situational awareness and supports faster, more informed decision-making in time-critical scenarios.

3.3 Intelligent sonar systems

Recent developments in sonar technology have integrated AI directly into sensing systems. Intelligent sonar platforms can automatically process acoustic signals, classify detected contacts and filter out background noise in real time.

These systems are especially effective in high-clutter environments, such as ports and coastal regions, where traditional sonar systems often struggle. By distinguishing between benign and suspicious acoustic signatures, intelligent sonar reduces operator workload and increases operational reliability.

3.4 Autonomous platforms and persistent surveillance

The adoption of autonomous underwater and surface vehicles represents a major advancement in maritime protection. These platforms enable continuous monitoring of large areas without requiring direct human involvement.

Autonomous systems can operate in hazardous or inaccessible environments, significantly reducing risks to personnel. When equipped with advanced sensors and AI-based processing capabilities, they can perform detection, classification and tracking tasks in real time.

Their ability to provide persistent surveillance makes them particularly valuable for protecting critical infrastructure and high-risk maritime zones.

3.5 Multi-modal sensing and data fusion

A key trend in recent technological development is the use of multi-modal sensing, where data from different sensor types are combined to improve detection performance.

Sonar systems provide robust detection capabilities in low-visibility conditions, while optical sensors offer high-resolution imagery when environmental conditions permit. By integrating these complementary data sources, multi-modal systems achieve greater accuracy and reliability than single-sensor approaches.

This fusion of data enhances situational awareness by providing a more complete representation of the underwater environment.

3.6 Distributed sensor networks

Another significant advancement is the deployment of underwater acoustic sensor networks, which enable large-scale and continuous monitoring through distributed sensing.

These systems consist of multiple interconnected nodes that collaboratively detect and track underwater objects. Recent research has focused on improving their energy efficiency through optimized communication protocols and lightweight processing techniques.

By maintaining high detection accuracy while minimizing power consumption, these networks support long-term deployment and are particularly suitable for protecting critical maritime infrastructure.

4. Conclusion

Recent technological advances have significantly reshaped underwater maritime protection, transitioning from traditional, operator-dependent methods to intelligent, integrated systems. The combination of AI-driven analysis, advanced sonar technologies, autonomous platforms and distributed sensor networks has greatly improved detection, classification and response capabilities.

These developments reflect a broader shift toward automation, integration and adaptability in maritime security. By focusing on the detection of physical objects and anomalies, modern systems provide a robust framework for addressing diverse and evolving underwater threats.

As research and innovation continue, these technologies will play an increasingly vital role in safeguarding maritime infrastructure, enhancing operational safety and ensuring security in complex underwater environments.

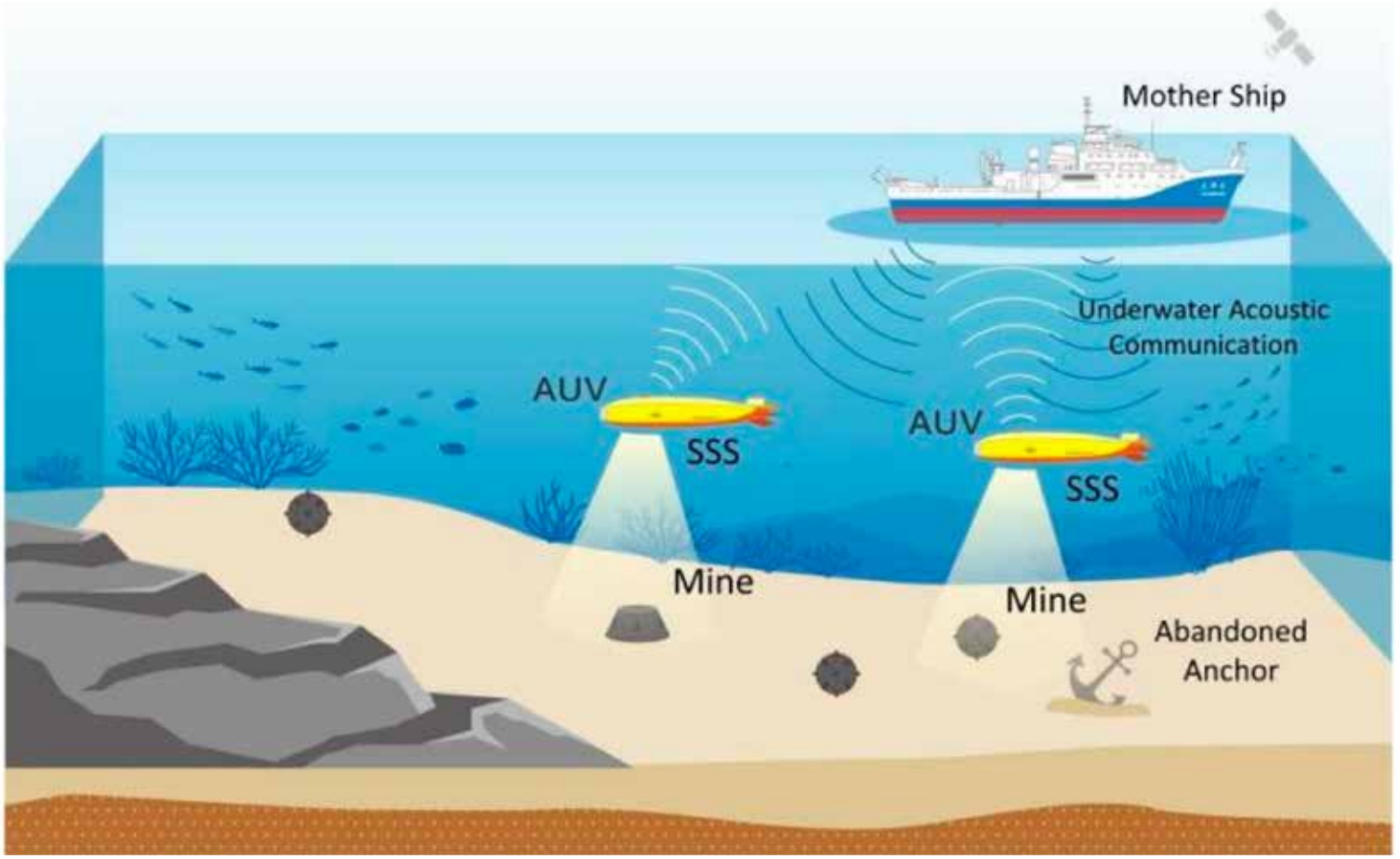


Figure 1: Underwater monitoring using autonomous vehicles (Source: https://www.mdpi.com/2077-1312/11/4/690)

Trends in the use of Ground Vehicle-Borne Improvised Explosive Devices

On 5 February 2026, DAESH Sahel (ISSP) conducted an up-armored suicide attack using a Vehicle-Borne Improvised Explosive Device (VBIED) against a Malian Army convoy near Menaka. According to the group's claim of responsibility, the up-armored vehicle was driven by an individual identified as "Abdul Rahman al-Ansari".

The first reported use of up-armored VBIEDs by DAESH Sahel took place on 19 June 2025 during the attack on Bani Banghou, Niger, where new tactics, techniques and procedures (TTPs) were observed. The migration of these TTPs suggests potential support or influence from DAESH West Africa Province (ISWAP).

The first use of up-armored VBIEDs by DAESH Somalia (ISS) was also documented in early February 2025, after Somali security forces intercepted an explosive-laden SUV fitted with additional armor protecting the engine compartment, windows and windshield.

In addition, other religiously motivated violent extremist organizations aligned with Al Qaeda are adopting similar TTPs. JNIM (Jama'at Nasr al-Islam wal Muslimin) demonstrated the use of up-armored suicide VBIEDs during the attack against a military base shared by Malian forces and Russian contractors in Ber, Mali, on 6 October 2024.

One of the most active groups employing VBIED TTPs in the region is the Baloch Liberation Army (BLA), which has even incorporated female suicide drivers into its operations, such as the VBIED attack against Pakistani forces in Noshki on 31 January 2026. In fact, the BLA currently leads the number of VBIED incidents recorded during 2026, followed by Fitna Al Hindustan (FAH).

At the same time, Syria and Yemen continue to experience recurring VBIED incidents during the first months of 2026.

Despite years of counterterrorism operations, DAESH remnants in Iraqi territory retain the capability to manufacture and employ VBIEDs, particularly in the Middle Euphrates River Valley. The VBIED attack against a police station in al-Mayadin, near Deir ez Zor, on 18 May 2025 serves as a clear example.

In Afghanistan, DAESH Khorasan Province (IS-KP) continues conducting VBIED attacks against local security forces, primarily using motorcycles or IEDs concealed inside buses. At the same time, some elements operating from Afghan territory are suspected of facilitating or planning VBIED attacks inside Pakistan.

However, the use of VBIEDs during 2025–2026 has not been limited to non-state actors. The Israeli Armed Forces (IAF) have reportedly employed obsolete M113 armored combat vehicles (ACVs) filled with explosives as improvised explosive platforms in Gaza and the West Bank. Similar practices have also been observed in Syria.

Drug cartels across the Americas are also progressively increasing their use of VBIED TTPs, both against government forces and rival criminal organizations. VBIEDs have additionally been employed by extremist radicals, such as in the attack against a fertility clinic in Palm Springs, California, in May 2025.

Examples of VBIED incidents can also be found in Colombia, such as the case in Belén de los Andaquíes, Caquetá, on 22 December 2025. Similarly, Mexico has witnessed multiple VBIED-related incidents, including the attack against Community Police facilities in Coahuayana, Michoacán State, on 6 December 2025.

Ecuador has also experienced VBIED attacks, such as the incident in Guayaquil on 15 October 2025, which was the latest in a total of five VBIED-related events recorded in the country during 2025.

Finally, Europe has not remained immune to the VBIED threat. The Ukrainian theater of operations has witnessed numerous tactical and criminal incidents involving both remotely controlled explosive-laden unmanned ground vehicles and emplaced VBIEDs. Such developments are unsurprising in a highly dynamic and adaptive combat environment.

Possibly related to the ongoing regional crisis, Russian Lieutenant General Fanil Sarvarov was reportedly killed following the detonation of an explosive-laden vehicle in southern Moscow on 22 December 2025.

Similarly, cases involving explosive-laden vehicles have also been identified within the European Union, primarily linked to criminal networks targeting rival groups, although not exclusively. For example, Dutch Police classified as a failed terrorist attack an incident involving a suspected VBIED that occurred in Dam Square, Amsterdam, on 3 April 2025.

Another recent VBIED-related case was the attempted attack against Italian journalist Sigfrido Ranucci on 16 October 2025 in Pomezia, near Rome.

In conclusion, although the use of IEDs concealed within ground vehicles is not a new phenomenon, the increasing sophistication and evolution of VBIED tactics, techniques and procedures in Africa represent a realistic threat to the Southern Flank of the European Union and the North Atlantic Treaty Organization.

VBIEDs are not only potential "weapons of mass destruction" capable of causing mass casualties and structural collapse, but also powerful psychological instruments intended to generate fear, intimidation and public terror.

REFERENCES

- X (former Twitter)
- Telegram
- Facebook
- LinkedIn
- VKontakte
- MATRIX/ELEMENT
- Reuters
- https://jamestown.org/red-fort-blast-brings-urban-operations-to-india/
- @HKaaman

Figure 1 – Captures of propaganda from the DAESH Sahel VBIED attack in Mali 05FEB2026 (Source: An Naba Newsletter 534)

Figure 2 – Capture from a propaganda video by DAESH showing a suicide up-armored VBIED in Niger (Source: X)

Figure 3 – Capture from a propaganda video by DAESH showing an up-armored VBIED in Puntland SOM FEB2025 (Source: X)

Figure 4 – Picture by JNIM showing an up-armored VBIED in Mali, October 2025 (Source: X)

Figure 5 – VBIED events in Raqqa SYR on 25 January 2026 and Sanna YEM on 21 January 2026 (Source: X)

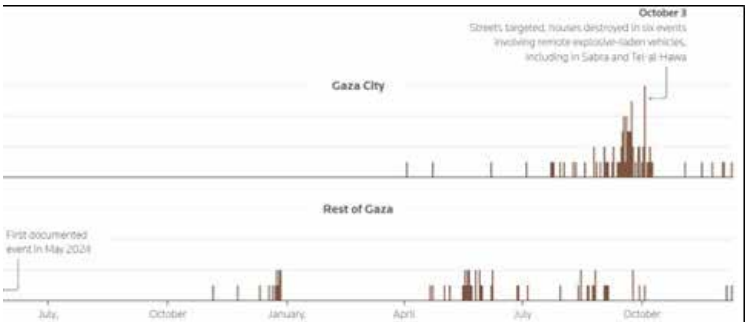


Figure 6 – Metrics on the use of remotely-controlled VBIED in Gaza 2024-2025 (Source: Reuters/ACLED)

Figure 7 – Examples of armored VBIED use (Source: X)

Figure 8 – Pictures from the VBIED found in Belén de los Andaquíes, COL 22DEC2025 (Source: Caracol Radio)

Figure 9 – Pictures from the VBIED incident in Guayaquil ECU 15OCT2025 (Source: Telegram)

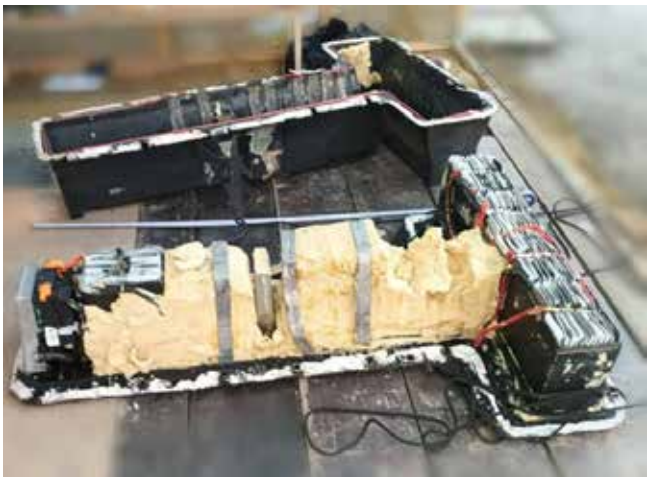


Figure 10 –VBIED on the battery compartment of an electric car seized near Crimean bridge 29OCT2025 (Source: www.9111.ru)

Figure 11 – DAESH manual on VBIED manufacture published in September 2025 (Source: MATRIX/ELEMENT)

NATO OTAN

Accredited COE

C-IED COE

CENTRES OF EXCELLENCE (COES) ARE INTERNATIONAL MILITARY ORGANIZATIONS THAT TRAIN AND EDUCATE LEADERS AND SPECIALISTS FROM NATO MEMBERS AND PARTNER COUNTRIES

MORE AT: nato.int

Could Transparent Battlefield host hybrid strategies?

Non-state Armed Groups dynamics update in Sahel, an overview on JNIM

NATO defines Hybrid Threat as "A type of threat that combines conventional, irregular and asymmetric activities in time and space" (NATO agreed term since 2018). There seems to be no doubt about the concepts conventional or irregular, but perhaps we should also establish the concept Asymmetric threat according to NATO definition as "A threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain a disproportionate result" (NATO agreed term since 2003).

In order to address this question, we will point at two premises while putting aside conventional and irregular activities. The first is that all the different actors have decided that they are de facto outside of the grey zone, so they are in an open and transparent conflict.

The second premise is to determine whether the so-called hybrid actions satisfy the primary characteristics of these actions, such as the set up of established red lines or non-linearity (being scalable) in both planning and execution, among other characteristics specified within the academic literacy.

Cognitive Environment (in the information domain)

Earlier this year, JNIM released some photos of a meeting in Timbuktu with various local authorities, intermediate military chiefs and academics, including Touaregs and other ethnic groups. Houssein Ghoulam, who defected from the Azawad Liberation Front to JNIM, is identified as a speaker in what appears to be a Key Leader Engagement activity.
Midway through January, JNIM published pictures of a variety of exercises conducted at its training camp in Timbuktu, including as shooting drills, fighter training and strengthening marches.

Not to mention that JNIM published recommendations to the Dogon militias (traditionally pro Malian Government) at the start of its expansion to stop the Mali government from adopting the militia model that was gaining traction in other neighboring countries. JNIM suggested that if militias wanted to fight against them, they should join the FAMa rather than organize as partners of the FAMa. By doing this, they would stop JNIM from viewing their hamlet and tribe as potential targets.

The future of defence is no longer defined solely by weapons or borders; instead, it is defined by cognition (Marsh, C, 2026 - The Defence Horizon Journal)

JNIM has established traffic controls, particularly for coach transportation, as it has got closer to the cities. In order to facilitate their transit, they posted on their social networks the layout to adopt (men in front, ladies behind), guaranteeing that the carriers who obeyed these instructions would not be viewed as "targets".

Disinformation

Following the summer of 2025, JNIM announced the creation of a new Katiba in Niger, where it started conducting guerrilla warfare in regions close to the Malian border as part of its expansion phase.

The question is raised because in the months that followed, there were multiple protests in Nigerian border towns that accused the Malian Armed Forces of failing to adequately defend the borders by permitting JNIM tactical cells to pass.

Did they try to orchestrate this expansion with already-existing units on Malian territory, or did they create a new Katiba in Niger?

Red Lines

It is noteworthy that JNIM has not attempted to subjugate Bamako, the capital, even though it is close by. The concentration of forces for this conquest probably resulted in exposure to the FAMa, which caused

significant losses, because of prior bad experiences (both in 2015 and in 2024). The red line has been set thus far: the conquest of Bamako will not be carried out.

Alternatively, these contingents may be used in other places, achieving a stronger presence and a greater number of actions seeking the benefit of hybrid techniques.

And this is in spite of the statement made at the beginning of January by Abu Yahya, regarded as JNIM's commander of operations, that they will concentrate on urban areas during the second phase of the conflict.

Economy

In addition to causing a severe scarcity that mostly affects civilian population, the blockade implemented by JNIM through the requisition and destruction of petroleum tankers near the cities and at the border ports they control has also severely damaged Malian economy.

Additionally, by disposing of this fuel, even going so far as to confiscate civilians, they have exploited a particular narrative of military abuse of power. In order to dispel this narrative, the government had to set up (and publicize) military supply points that were distinct from civilian supply points.

Adverse unintended (or unplanned) effects

A small number of JNIM personnel have defected since the release of Joumaa Bin Maktoum, a member of the Emirati royal family, which would have required the payment of a historic ransom, both in cash and military supplies. This could have resulted in low-level infiltrations by ISIS due to their increased access to resources.

The only thing that caused anxiety and activity among the nations involved in the most likely delivery routes (not to mention in the Malian Junta) was the information environment's distribution of the ransom payment in war material.

Sadou Samahouna, a senior commander and the brother of Abu Hanifa, the JNIM Emir for Niger, led a defection and afterwards, he made statements on social media claiming that the primary cause of his decision was the Shura of JNIM's growing laxity or flexibility in enforcing Sharia.

This clarifies, at least in a small part, the conundrum raised by some analysts on whether the massive expansion would encourage a loss of internal cohesiveness.

Conclusions

We can prove that JNIM is using hybrid tactics on a transparent battlefield, even though it is far from the definitions of hybrid warfare in the Western sense.

They are not the only actors, though. A "retouched" photo of a Touareg contingent flying both the Ukrainian flag and the Touaregs' own flag surfaced on social media and in Ukrainian press following the battle of Tinzawatene in 2024 (the largest disaster known to the FAMa and the Russian Wagner Group). This image even caused several countries to sever diplomatic ties.

Furthermore, images of Azawad Liberation Front UAS operators donning green T-shirts from the Ukrainian regular uniform have lately surfaced.

The cognitive study of current networks in the operational environment, including the hybrid strategies that could be implemented in the catalogue of these networks' capabilities, is urgently needed if we take into account the three stages of the Attack the Networks (AtN) process (understanding the network, identifying intelligence and attacking the network). This is the only way these networks could be targeted comprehensively and with a chance of success.

Ukraine - Trends in Explosive-Laden drone designs

In a threat environment in which homemade rotary-wing first person view (FPV) drones are dominating the scenario, Russian forces developed a low-cost fixed-wing model based on plywood, foam and aluminum: the "MOLNIYA" ("молния"/Blitz), from late 2024 on.

The single electric engine MOLNIYA and its most developed two-rotor version MOLNIYA-2 are cheap, modular, easy to assemble, low signatured and flexible platforms capable of getting transformed into munition dropping, vehicle-borne IED, decoy, relay, FPV drone transporter and intelligence, surveillance and reconnaissance unmanned aircraft systems.

In due answer to the Russian production of MOLNIYA series, and through reverse engineering, a Ukrainian engineer has developed a sort of copy of the MOLNIYA-1 called as "BLYSKAVKA" ("БЛИСКАВКА ,"lightning"): it would provide the Ukrainian side with a similar easy-manufactured and multitask capability to that of the Russians.

In accordance with the reported data, the BLYSKAVKA drone allows a maximum flight range of about 40 kilometers and can reach altitudes of up to 2,000 meters, while it can carry a payload of up to 9 Kg.

At a very first sight, the improvised munition loaded by the shown BLYSKAVKA drone could cause some confusion making analysts think that it could be some sort of field artillery shell. But a deeper analysis shows the following indicators:

- There is a threaded bottom piece, which is not consistent with an artillery shell, but it is with the upper portion of a mortar grenade body.
- In comparison with a human holding the drone, the diameter of the munition body could be of about 80-90 mm.
- We could read "AMM LO..." and "... 74 AMM".
- The top portion of the improvised munition is consistent with the tail connector of a mortar grenade but covered with a sort of green cap.

All those indicators clearly identify the improvised munition based on an 81 mm mortar grenade body turned 180°: plastic explosive is allocated inside its usual fuse hole and a green cover is emplaced over the tail connection.

REFERENCES

- X (former TWITTER)
- Telegram
- www.static.nv.ua
- www.united24media.com
- www.defence-ua.com
- www.censor.net
- www.dev.ua
- www.worthpoint.com
- www.resonantnews.com

Figure 1 – Russian low-cost MOLNIYA-1 UAS (Source: www.censor.net/www.resonantnews.com)

Figure 2 – MOLNIYA fitting a KZ-6 demolition charge & optic fiber controlled MOLNIYA-2 (Source: X/www.defence-ua.com)

Figure 3 – MOLNIYA-2 UASs with STARLINK antenna and loading FPV UAS (Source: www.static.nv.ua/www.united-24media.com)

Figure 4 – MOLNIYA 2 with IEDs based on TM-6 landmine and PG warheads (Source: www.dev.ua/Instagram)

Figure 5 – BLYSKAVKA UAS (Source: Instagram)

Figure 6 – Details of the improvised munition of the BLYSKAVKA UAS (Source: Instagram)

Figure 7 – Body of a M374A1 mortar grenade (Source: www.worthpoint.com)

Artificial Intelligence-Driven C-IED: Empowering the full spectrum of response

Modern warfare has transitioned swiftly from a contest of physical mass to a competition of cognitive speed. As outlined in recent strategic forecasts toward 2045, Artificial Intelligence (AI) is no longer a technical elective, but a doctrinal imperative that redefines the human role in conflict.

In the C-IED discipline, AI fundamentally compresses the engagement timeline: on the one hand, it enables adversaries to automate the IED lifecycle (from procurement to autonomous delivery) while on the other, it empowers C-IED forces, across the three doctrinal pillars, to disrupt threats before they materialize.

The contemporary battlespace, an operational testbed for AI integration, is witnessing a radical shift toward data-centric ecosystems. Evidencing this paradigm shift, Ukraine's Delta and Avengers platforms demonstrate how AI-driven, cloud-native architectures enable real-time situational awareness and decentralized command under contested conditions. This acceleration of the sensor-to-shooter cycle provides a case in point for C-IED, proving that efficacy lies in fusing multi-source intelligence into decision advantage.

Regarding the emergence of Unmanned Systems as Autonomous Vectors, the evolution of First-Person View (FPV) drones (i.e.: airborne IEDs) into platforms capable of inertial navigation and autonomous terminal engagement represents a direct response to electromagnetic warfare (EW) saturation. By enabling 'on-edge' processing, AI allows these systems to maintain a consistent target lock despite severe link degradation or active jamming.

From a C-IED perspective, this technological shift transforms the fundamental nature of the threat from a traditional static device into a mobile, semi-autonomous weapon system capable of independent terminal maneuvers. Simultaneously, against the aforementioned technological developments, Artificial Intelligence can also serve as a cross-cutting enabler across the entire C-IED functional spectrum.

In the **Attack the Networks (AtN)** pillar, AI-driven analytics could, for instance, revolutionize the exploitation of the IED system lifecycle. By integrating multi-source data, such as social media (OSINT) and illicit procurement patterns, algorithms can identify non-obvious links within insurgent cells. These capabilities serve as examples of how machine learning can transition C-IED from a reactive posture to a proactive disruption of the adversary's financial and logistical support structures.

Regarding **Defeat the Device (DtD)**, the integration of AI into tactical operations offers significant potential for enhancing identification, standoff detection and neutralization. For instance, AI-enabled sensors can drastically mitigate the cognitive load on EOD operators by automating pattern recognition in high-clutter environments. Furthermore, current operational deployments illustrate how autonomous systems also augment Technical Exploitation (TE), shifting the paradigm toward greater safety and precision during the final engagement.

Finally, in the **Prepare the Force (PtF)** line of effort, AI-driven simulation and wargaming can provide high-fidelity training environments where adaptive learning systems modify threat scenarios in real-time based on trainee performance, ensuring that C-IED enablers are conditioned against the most current adversary Tactics, Techniques and Procedures (TTPs) through a customized and evolving pedagogical approach.

In conclusion, AI will not replace the Improvised Explosive Device Disposal (IEDD) operator. However, the operator augmented by AI will inevitably supersede the one who is not. Achieving cognitive superiority must remain our definitive end state, ensuring that the Allied response is faster, more precise and more resilient than the evolving explosive threat.

References & Further Reading

Bondar, K. (2026). How Russia Is Reshaping Command and Control for AI-Enabled Warfare. Wadhwani AI Center. Center for Strategic and International Studies (CSIS).

C-IED Centre of Excellence (2024-2025). "Emerging and Disruptive Technologies: Artificial Intelligence in Multi-Domain Operations." CHESSBOARD Magazine, Issues 01-04. NATO C-IED COE.

Grey dynamics (2024). Network-centric Warfare in Ukraine: The Delta System [online]. Available: https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/

Ministry of Defense of Ukraine (2024). Delta: The Cloud-Native Situational Awareness Platform and the 'Avengers' AI Integration in Modern Warfare. Official Strategic Communications Division. [Online]. Available: https://www.mil.gov.ua/ (Referencing the successful integration and testing during NATO CWIX 2024 exercises).

Moser, R. (2026). "Constructing AI's Future." The Power of ERDC Podcast, Episode 42. U.S. Army Engineer Research and Development Center. [Online]. Available: https://poweroferdcpodcast.org/42-artificial-intelligence/

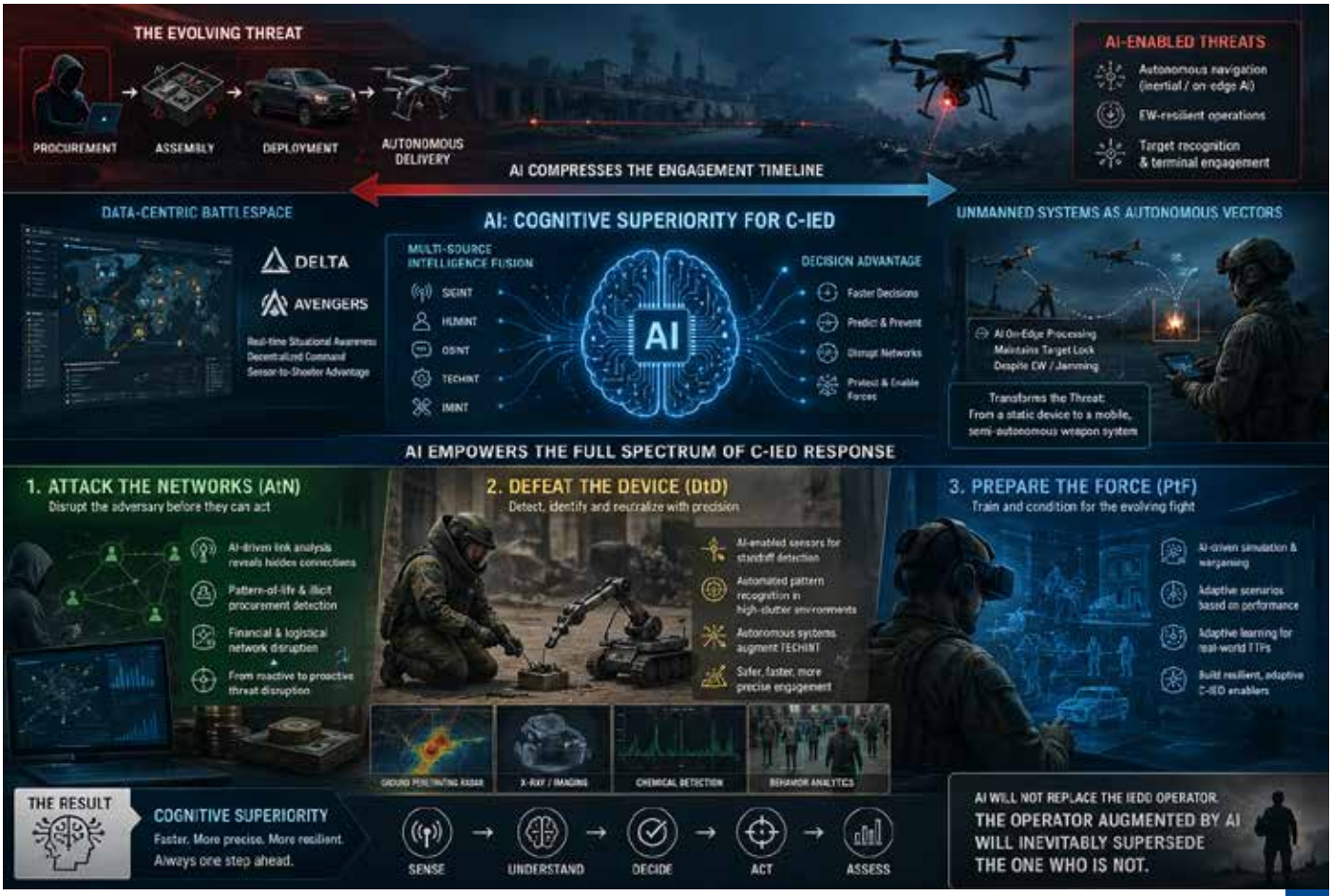
NATO Science & Technology Organization (2025). Science & Technology Trends 2025-2045: Volume 1. NATO STO.

U.S. Department of Defense (2023). Data, Analytics and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage. DoD Chief Digital and Artificial Intelligence Office (CDAO).

Villanueva López, C. D. (2026). Artificial Intelligence and Warfare through 2045: Redefining the Human Role in Conflict. Ejércitos Digital Magazine (English Edition/ Translation).

War on the Rocks (2024). Quality Has a Quality All Its Own: The Virtual Attrition Value of Superior-Performance Weapons. [Online]. Available: https://warontherocks.com/2024/06/quality-has-a-quality-all-its-own/

Photo: chatGPT



Ideas for a smart implementation of C-IED at NATO and multinational HQs

Introduction

Counter-Improvised Explosive Devices (C-IED) can no longer be understood mainly through the land-based roadside bomb that dominated NATO operations in Iraq and Afghanistan. The problem set is now broader, more adaptive and increasingly linked to new vectors, especially unmanned systems. Explosive effects can be delivered, enabled or supported by small, unmanned, aerial, surface and subsurface systems, while components and triggering architectures can be distributed across the theatre.

At the same time, information recovered from devices, launch platforms, digital media and associated materiel has gained operational value. Technical Exploitation (TE) is therefore central to understanding adversary design, supply chains, tactics, signatures and adaptation.

This evolution also has a multidomain dimension. The threat is not only land, maritime or air in its physical expression; other domains may enable, conceal, direct or amplify it. Digital enablers, information effects and other cross-domain mechanisms increasingly shape how such threats are prepared and employed.

This matters because NATO's current and likely future operations, especially collective defense and Article 5 scenarios, are no longer defined by IED dominance in the way previous campaigns were. IED is often no longer the single most visible or decisive threat. That does not mean the threat has disappeared. It has evolved and grown closer to unmanned systems and other emerging vectors.

NATO structures must therefore evolve as well. C-IED must be integrated in headquarters at all levels, but especially at operational and higher tactical level, where force protection, threat assessment, intelligence fusion, targeting priorities, information activities, operational assessment and exploitation outputs must be linked into a coherent staff process. The question is how to position it so that it remains

relevant, preserves specialist expertise and enables proactive action against adaptive threat networks.

What a smart implementation should achieve

Any smart implementation model for C-IED should meet five conditions. First, it should be threat-driven rather than legacy-structure driven. Second, it should preserve enough C-IED identity and specialist expertise to avoid dilution. Third, it should support Attack the Networks by moving the staff from event response to adversary-system disruption. Fourth, it should connect naturally with TE, intelligence, current operations, planning, force protection, information activities, operational assessment and targeting. Fifth, it should scale across levels of command so tactical outputs can feed operational decision-making and vice versa.

Viewed against those criteria, three organizational approaches are plausible. The first places C-IED within a broader Counter Emerging Threats construct inside a Protection Branch under J3/G3. The second retains C-IED as an independent staff element within J3/G3, outside Protection. The third places it inside the engineer architecture, normally within JENG. Each model can function in some context, but each one constrains the discipline differently.

Model 1: C-IED within a Counter Emerging Threats construct under Protection Branch (J3/G3)

The first model groups C-IED with closely related disciplines such as counter-Class I UAS, counter-USV, counter-UUV, counter-UGS and TE under a broader Counter Emerging Threats (C-ET) construct. Located in a Protection Branch under J3/G3, it is explicitly threat-driven. Its logic is that NATO headquarters increasingly face converging threats that exploit cheap technology, distributed access, low signatures and rapid adaptation.

Its principal advantage is integration. C-IED would no longer be treated as a standalone problem derived from past campaigns, but as part of a broader set of emerging threats. The relationship with TE would also be stronger. Material recovered from an IED event, a UAS payload, an improvised launch device or a maritime unmanned platform can all produce exploitable information on sourcing, design practice and network relationships. TE thus becomes a common enabler rather than an activity tied narrowly to one discipline.

Model 1 is also the most naturally multidomain. It can integrate threats expressed across land, maritime and air vectors while also accounting for other domains that support targeting, command and control, deception, logistics or influence. Because it is threat-driven, it is better placed to absorb that complexity than models tied to narrower functional ownership. Properly designed, it also offers the best basis for preserving and expanding Attack the Networks across related disciplines.

The challenge is cultural. Protection communities have traditionally been more comfortable with defensive functions. A C-IED/C-ET construct inside Protection therefore requires clear recognition that one essential component of the function remains offensive in nature: proactive network attack. If that is not understood and safeguarded, the structure may preserve only the protection-facing side of the discipline. Even so, this model offers the strongest long-term logic for operational and higher tactical headquarters, provided C-IED expertise and ownership of network-attack functions are explicitly protected.

Model 2: Independent C-IED staff element within J3/G3 outside Protection Branch

The second model preserves C-IED as a distinct staff function directly under J3/G3 but outside Protection. At first sight, this appears balanced. It keeps the discipline visible and doctrinally legible, and it preserves a focal point for policy, planning, incident understanding, mitigation measures and liaison with supporting enablers.

Its main danger, however, is structural fragility in new NATO operations, particularly Article 5 scenarios. In such contexts, headquarters may judge other functions more urgent and use C-IED personnel to reinforce broader operational structures. The discipline may not disappear formally, but it can languish and dilute in practice. Model 2 can therefore become a pathway to gradual institutional erosion.

That erosion would affect more than C-IED alone. If the discipline remains isolated and weak, adjacent counter-unmanned disciplines are also less likely to benefit from the proactive logic that has traditionally distinguished mature C-IED approaches. The result is a stronger focus on platform defeat and a weaker focus on disruption of adversary systems. Model 2 may therefore preserve C-IED identity in the short term, but it also carries a significant risk of progressive irrelevance.

Model 3: C-IED staff element within JENG / engineer division

The third model places C-IED inside the engineer structure, where the discipline historically found an institutional home in many headquarters. This arrangement benefits from familiarity and a natural connection with survivability, mobility support, routes, field fortification, EOD and aspects of explosive hazard understanding. It is also probably the model under which the discipline is most likely to survive institutionally, because JENG provides a stable functional home.

Yet survival comes at a cost. When nested inside JENG, C-IED is more likely to be framed around Defeat the Device than around the broader offensive logic of Attack the Networks. This does not mean engineer structures cannot support proactive activity, but the institutional gravity of JENG tends to pull the discipline towards protection and technical response. As a result, the offensive, intelligence-led and disruption-oriented character that should define mature C-IED risks being weakened.

That is the central limitation of Model 3. It preserves the discipline as an identifiable function, but at the price of losing part of its essence. In practice, C-IED may continue to exist while becoming narrower, more reactive and less influential across the headquarters.

Conclusion

The present challenge is not simply where to place C-IED on an organizational chart. It is how to adapt a discipline to a changing threat. NATO no longer operates in an environment where the IED threat is as dominant as it once was, but that should not be mistaken for declining relevance. The threat has evolved through new vectors, stronger multidomain linkages and the growing exploitation value of recovered material. As a result, C-IED must evolve as well.

If the priority is future relevance, multidomain integration and a genuinely threat-driven design, Model 1 is the strongest. It aligns best with the reality that IED effects, unmanned systems, TE outputs and other enabling domains increasingly overlap. It also provides the best institutional basis for extending Attack the Networks beyond traditional C-IED boundaries, although it requires Protection communities to accept that an essential part of the function remains offensive in character.

If the priority is to preserve a recognizable C-IED identity with minimal reorganization, Model 2 is understandable, but it carries the risk that the function will gradually lose relevance as personnel are absorbed elsewhere.

If the priority is institutional continuity, Model 3 is the safest home, but it does so largely by centering the discipline on Defeat the Device and reducing its proactive character. The decisive issue, therefore, is not whether C-IED survives as a label, but whether it retains its proactive, threat-driven and operationally relevant character within NATO headquarters as both the threat and HQ structures evolve.

Summary comparison

Model	Main strength	Main risk	Operational implication
Model 1 J3/C-ET	Most threat-driven and multidomain	Protection culture may underweight offensive logic	Best basis for spreading Attack the Networks across related disciplines
Model 2 J3/C-IED	Keeps C-IED visible in theory	Can be hollowed out in Article 5-type operations	Risks isolating C-IED and denying counter-UxS disciplines the proactive mindset
Model 3 JENG/C-IED	Most likely to preserve the C-IED label	Pulls C-IED towards Defeat the Device	Keeps the function alive, but weakens its offensive essence

Ab invisibilibus ad visibilia

(From the invisible to the visible)

Understanding Document and Media Exploitation in modern operations

"Life and death appeared to me ideal bounds, which I should first break through, and pour a torrent of light into our dark world."

Mary Shelley, Frankenstein, Chapter 4

Introduction: Making the inert speak

In Mary Shelley's Frankenstein, a scientist assembles lifeless, silent parts, fragments of bone and tissue that, on their own, carry no meaning. Then comes the current: the inert becomes animated and the creature speaks. Document and Media Exploitation (DOMEX) works on the same principle. On any modern battlefield, or crime scene, the mobile phone in the evidence bag, the hard drive from the safe house and the crashed UAV from the field, all these objects, are silent, Shelley's disconnected limbs. DOMEX is the current that runs through and forces them to speak. Forensic acquisition, metadata extraction, timeline reconstruction and link analysis: each step is a volt that transforms inert physical evidence into something that feeds the intelligence cycle, support the targeting process and protects forces in the field.

DOMEX has no single operational home. From the close battle of high intensity armed to the courtrooms of multi-jurisdictional organized crime prosecutions, from maritime interdiction to the contested digital infrastructure of hybrid warfare, the same current runs in this article through twelve distinct operational environments, covering conflicts of today and the technological frontiers of tomorrow. In every one of them, the central demand is the same: trained operators and analysts, standardized procedures and the analytical depth to extract data and metadata not only from what adversaries choose to record, but from what they do not know they are broadcasting. Each of them begins with an inert object, a phone, a hard drive, a UAV, and ends with a commander informed, a network dismantled or a criminal convicted. The electricity is DOMEX.

The four "domains" of DOMEX

DOMEX encompasses four specialized exploitation disciplines, each targeting a distinct category of collected exploitable material (CEM). Together, they make up a comprehensive framework for turning physical evidence (data and metadata) into actionable intelligence. The most impactful DOMEX operations are rarely single domain: they are coordinated efforts in multi-domain exploitation, where a document confirms a phone record, a flight log confirms a cache location and a hard drive reveals the network that connects them all.

Domain	Primary Material	Core Methods	Outputs
Document Exploitation (DOCEX)	Physical documents, identity documents, maps, printed & engraved materials…	Content analysis, forensic document examination, handwriting analysis, latent print recovery…	Network link charts, travel pattern analysis, identity verification, order of battle assessments…
Media Exploitation (MEDEX)	Computers, hard drives, USB drives, memory…	Forensic imaging, file system recovery, deleted data retrieval, metadata analysis, timeline reconstruction, encryption bypass…	Geolocation data, authorship attribution, communication maps, financial transaction traces, targeting packages…
Cellular Exploitation (CELLEX)	Mobile phones, smartphones, SIM cards, tablets…	Forensic extraction (including lock bypass), call log analysis, GPS geotag extraction, messaging thread recovery, financial app analysis…	Communication network maps, movement timelines, associate identification, strike coordinates, sanctions evidence…
Unmanned Systems (UxS) Exploitation	UAVs, UxS controllers, antenna, recovered UAS components…	UAV internal memory acquisition, flight controller memory extraction, SD card forensics, metadata analysis, firmware examination…	Supply route back-tracing, staging area identification, operator attribution, procurement network mapping, pre-attack planning evidence…

Table 1. DOMEX specialized exploitation areas (included but not limited to)

The procedural discipline applied within each domain, from collection through forensic acquisition, extraction, analysis and reporting, determines not only the operational value of the resulting intelligence, but also its admissibility as evidence. An extraction performed without a forensic write-blocker may alter timestamps, destroying evidentiary value. A device acquired without cryptographic hashing cannot be proven unmodified. Chain of custody documentation that is incomplete may invalidate all material derived from a CEM. In each case, failure is not technical: it is procedural. Structured DOMEX training is therefore not a luxury but an operational necessity. The operator who understands why a hash value must be recorded will apply the procedure correctly under pressure, in degraded conditions, with a damaged device, in a foreign language environment. The analyst who understands the limits of metadata will produce assessments that are both honest and operationally reliable.

Figure 1. From Inert Device to Actionable Intelligence. The DOMEX Flow

Operational Environments: Overview

The following table provides a reference across all twelve environments covered in this article. Environments are categorized as Current (actively relevant today), Current/Emerging (present but rapidly evolving) or Future (anticipated within the next decade). DOMEX priority reflects the assessed criticality of exploitation capability within that environment.

Operational Environment	Type	Primary DOMEX Domains	Priority
High-intensity Armed Conflict	Current	MEDEX, CELLEX, DOCEX, UxS Exploitation	Critical
Counterterrorism / CT Operations	Current	DOCEX, MEDEX, CELLEX	Critical
Stabilization & COIN	Current	DOCEX, MEDEX, CELLEX	High
Battlefield Evidence	Current	DOCEX, MEDEX, CELLEX	Critical
Border Control & Migration	Current	DOCEX, CELLEX	High
Cyber-Physical / Hybrid	Current/Emerging	MEDEX, CELLEX, UxS Exploitation	High
Maritime & Littoral	Current/Emerging	DOCEX, MEDEX, UxS Exploitation	High
Large-Scale Combat Operations	Future	All domains + AI triage	Critical
Space & Satellite Systems	Future	UxS Exploitation, MEDEX (firmware)	Emerging
Autonomous / AI-Enabled Threat	Future	MEDEX, CELLEX, UxS Exploitation	Critical
Quantum-Encrypted Networks	Future	MEDEX, CELLEX (post-quantum)	Emerging
Smart Cities / IoT Environments	Future	DOCEX, MEDEX, CELLEX	Emerging

Table 2. DOMEX Operational Environments: Type, Domains and Priority Level

Current Operational Environments

1. High-intensity armed conflict

High-intensity conventional conflict, as seen in Ukraine, Iraq and Syria, generates DOMEX opportunities at massive scale across battlespaces. All four domains (DOCEX, MEDEX, CELLEX and UxS Exploitation) are simultaneously relevant. Smartphones and military devices provide near-real-time intelligence on enemy disposition and command, captured documents reconstruct order of battle and recovered UAVs show reconnaissance priorities. The intelligence cycle runs in hours, requiring fast triage and analyst effort. Key challenges include time pressure, volume overload, management of damaged equipment and adversaries actively counter DOMEX measures through data wiping and deliberate deception. Despite these challenges, DOMEX delivers precise targeting data, enemy intent, and logistics intelligence that no other source can provide. Exploitation material also helps support post-conflict war crimes accountability.

⚠ Challenges	✓ Benefits & Intelligence Value
• Extreme time pressure: tactical intelligence has a shelf life measured in hours • Volume overload: mass seizure events generate material faster than teams can process • Adversary counter-DOMEX: data wiping, device destruction, deliberate deception, USB killers	• Real-time tactical intelligence on force disposition, movement plans, and command contacts • Order of battle reconstruction from captured orders, maps, and identity documents • GPS-precise targeting coordinates from geotag metadata and UAV waypoint data

2. Counterterrorism

Counterterrorism (CT) is the environment where DOMEX has achieved the most documented intelligence successes, from Abbottabad to Mosul. Non-state adversaries depend heavily on commercial digital technologies for planning, coordination, financing and propaganda. MEDEX and CELLEX dominate CT exploitation, with the smartphone being the single richest intelligence source. A defining feature of CT DOMEX is its accumulative nature, gradually building persistent analytical databases over months and years. Exploiting a single device can gradually map entire adversary networks across multiple operations. Encrypted messaging apps and social media platforms are primary targets for exploitation. Unlike high-intensity conflict, CT exploitation is less time-critical but more network-focused. Results feed continuously into long-term analytical frameworks rather than immediate tactical decisions. This sustained, layered approach makes CT DOMEX uniquely effective at taking apart covert organizational structures.

⚠ Challenges	✓ Benefits & Intelligence Value
• End-to-end encryption and full-disk encryption significantly limit accessible data • Remote wipe capabilities: suspects configure devices for destruction upon capture • Speed vs. thoroughness tension: time-sensitive targets require immediate intelligence while forensic rigor demands methodical processing	• Network mapping: messaging histories and contact databases reconstruct terrorist cell structures • Financial intelligence: mobile banking records and cryptocurrency wallet data trace funds from sponsors to operational cells • Geolocation intelligence: GPS metadata from photographs places network members at safe houses and planning meetings

3. Stabilization & Counterinsurgency

Counterinsurgency (COIN) and stabilization operations represent a slower, population-centric environment where DOMEX serves both intelligence and governance purposes. Exploitation targets not only armed groups but also their support networks, financial infrastructure and propaganda elements. Examples include operations across Afghanistan, the Sahel and the Lake Chad Basin. DOCEX plays a comparatively larger role here, as insurgents frequently rely on printed materials and handwritten records. The legal and ethical complexity is among the highest of any operational environment, particularly when it comes to non-combatant data.

4. Battlefield Evidence (BE)

The law enforcement environment subjects DOMEX outputs to the most rigorous external control of any operational context. Operation Eureka against the 'Ndrangheta in 2021 showed how DOMEX can underpin prosecutions across multiple jurisdictions and hundreds of defendants. Every procedural decision during exploitation is potentially reviewable by a court, fundamentally shaping how exploitation is conducted. MEDEX and CELLEX are dominating, focusing on smartphones, laptops and encrypted storage devices. Cryptographic chain of custody and forensic imaging protocols are not optional but essential. Tamper-evident storage and strict procedural compliance determine whether exploitation results can be used as battlefield evidence. This environment demands the closest possible integration between technical exploitation capability and legal expertise.

⚠ Challenges	✓ Benefits & Intelligence Value
• Evidentiary standard requirements: every acquisition, storage, and analysis step must withstand cross-examination • Chain of custody integrity: any gap from seizure to courtroom may render all derived evidence inadmissible • Legal framework variation: admissibility standards differ significantly across EU, US, and other jurisdictions	• Prosecution-grade evidence: forensically acquired DOMEX provides legally admissible proof of presence, communication, and intent • Financial crime exposure: cryptocurrency wallet data, banking app records, and deleted transaction histories trace laundering networks • Deleted content recovery: material wiped from visible application layers (as in Op. Eureka) defeats the most common evidence-destruction countermeasure

5. Border control & migration

Border control and migration management represent a high-volume, legally sensitive and analytically demanding DOMEX environment. DOCEX and CELLEX are the main domains, focusing on identity documents, travel records and mobile phones. Key intelligence products include smuggling network mapping, document fraud pattern analysis and identification of criminal or extremist individuals within migration flows. The legal framework is highly complex, cutting across immigration law, data protection regulations and international refugee law. Effective border DOMEX requires close coordination between intelligence, law enforcement and legal representatives, and sophisticated triage systems to identify priority targets within large populations.

Current/Emerging Operational Environments

6. Cyber-Physical / Hybrid

Hybrid warfare deliberately combines conventional military action, information operations, cyber-attacks, economic pressure and proxy forces below the threshold of declared conflict. This creates a uniquely complex DOMEX environment, as seen in eastern Ukraine pre-2022, the Baltic states and contested spaces across Africa and the Middle East. The most distinctive analytical challenge is linking activity to state actors rather than non-state proxies, requiring advanced metadata analysis and cross domain correlation well beyond standard exploitation practice. Hybrid DOMEX demands the highest level of analytical sophistication and inter-agency coordination of any operational environment.

7. Maritime & Littoral

Maritime DOMEX covers counter-piracy, counter-narcotics, sanctions enforcement and maritime irregular warfare across a challenging operational environment. The physical difficulties of at-sea exploitation, the jurisdictional complexity of international waters and rich intelligence potential define this context. DOCEX plays an unusually prominent role compared to other environments, with ship manifests, charts, bills of lading, crew documentation and navigation logs collectively reconstructing route, cargo and ownership networks. The increasing use of unmanned surface vessels by state and non-state actors makes UxS exploitation a growing priority. Jurisdictional complexity in international waters creates significant legal challenges around seizure authority and evidence admissibility. The combination of physical and digital exploitation makes maritime DOMEX uniquely comprehensive in reconstructing adversary logistics chains.

Future Operational Environments

The following environments are defined by technologies already in development. Some are beginning to emerge now, but their full impact on DOMEX will be felt most strongly over the next ten years. Preparing for them is not optional; it is an institutional obligation.

8. Large scale combat operations

Large scale combat operations (such as a NATO Article 5 scenario) will generate DOMEX requirements and opportunities at a scale qualitatively different from anything seen in CT or COIN contexts. The conflict in Ukraine has given a partial preview: both sides have conducted systematic exploitation of captured equipment, vehicles and personnel, with results directly shaping tactical and operational decisions. Mass collection events (command posts, destroyed vehicle columns, large scale prisoner capture, etc.) will generate volumes of CEM that overrun the capacity of traditionally organized DOMEX capabilities. The integration of artificial intelligence for triage, translation and pattern recognition will move from desirable capability enhancement to operational necessity. Simultaneously, peer adversaries will apply counter-DOMEX at scale: systematic data destruction, device booby-trapping and deliberate deception operations designed to push false intelligence into exploitation process.

9. Space & Satellite systems

Space has become a contested operational domain. UxS exploitation methods developed for UAVs apply directly to the recovery and exploitation of satellite ground terminals, control systems and, in future scenarios, recovered orbital debris. The firmware, communication logs and configuration data stored in satellite ground stations represent high-value MEDEX targets. As adversaries increasingly rely on commercial satellite communications for military operations (as seen in Ukraine), the exploitation of satellite-linked devices and terminals becomes a tier-one intelligence priority.

10. Autonomous /Artificial Intelligence enabled threat

The proliferation of autonomous and AI-enabled platforms is creating a new category of exploitable material. Unlike conventional digital devices, autonomous systems contain operational intelligence embedded not in communications and documents but in their trained models, decision logic, sensor data and mission history. DOMEX applied to recovered autonomous platforms will need methodological innovation to extract and interpret this new type of data and metadata. Within the decade, recovered autonomous ground vehicles, underwater drones and AI-directed cyber tools will join the exploitation inventory, demanding a fusion of. UxS exploitation methodology, reverse engineering and machine learning expertise that does not yet exist as an organic DOMEX capability.

11. Quantum encrypted networks

The progressive deployment of quantum key distribution and post-quantum cryptographic algorithms by state actors presents a long-term challenge to DOMEX capabilities that depend on the ability to access encrypted content. The DOMEX response to quantum encryption is unlikely to be primarily technical: it will be procedural. The intelligence value of DOMEX in a post-quantum encryption environment will move further away from content exploitation toward metadata exploitation, physical device analysis and the exploitation of the endpoints (the devices and operators) before or after encryption occurs. The fundamental principle remains: no encryption protects metadata and no encryption protects content on a device that has been physically seized before it is locked.

12. Smart cities / Internet of Things environments

The progressive deployment of Internet of Things (IoT) infrastructure (smart city sensors, connected vehicles, wearable devices, home automation systems and industrial control networks) is creating an environment in which an individual's activities are recorded across dozens of simultaneous data streams. A threat actor operating in a smart city environment leaves traces across building access systems, vehicle sensors, mobile payment infrastructure and personal wearable devices that together reconstruct activity in more detail than CCTV ever could. The forensic exploitation of smart devices already features in law enforcement investigations; the extension of these methods to military and CT contexts is a question of time. The challenge is not finding the data but developing the legal, technical and analytical frameworks to access and exploit it.

Conclusion: The creature must be trained

Mary Shelley's scientist did not create life from nothing. He assembled fragments, applied the current and forced the silence to speak. DOMEX follows the same principle. Across the twelve operational environments presented in this article, the logic is always the same: a phone, a hard drive, a ship's manifest, a recovered UAV, each one silent until the current of DOMEX runs through it. What changes between a contested battlespace in Ukraine, a border crossing in the Mediterranean, a maritime interdiction in the Gulf of Aden and a courtroom in Calabria is not the principle but the pace, the legal framework and the technical sophistication required.

The seven current environments show that DOMEX is a core operational capability, present across the full spectrum of modern conflict and security activity. The five future environments confirm that the discipline's complexity will only be deeper. Adversaries will not stop generating exploitable material; they will simply make it harder to reach. The most decisive intelligence has consistently come not from visible content but from metadata: the timestamps, geotags, cell tower logs and cross-device links that adversaries unknowingly generated.

Shelley's creature, once animated, demanded to be understood. DOMEX demands the same: not just the tools to unlock devices, but trained DOMEX operators who understand why procedures matter, and DOMEX analysts who can think about what the data and metadata means and the importance of it for the intelligence community. The current is only as powerful as the professional who guides it.

The battlefield is increasingly digital. The information is already there, waiting in the inert and DOMEX is what makes it speak.

PREPARE!

COURSES & TRAINING

Strengthening WIT capabilities: The Trainer Developer Course and the Review Workshop are building the future of WIT

The continuous evolution of the Weapons Intelligence Team (WIT) capabilities remains a cornerstone of NATO's Counter-IED (C-IED) effort. With rapidly changing threat environments, new technologies and the growing need for interoperability among the Alliance, the development and refinement of WIT training have never been more crucial.

The recent execution of the WIT Trainer Developer Course (WIT TDC) in December 2025 and the WIT Review Workshop in January 2026 reflect the Centre´s commitment to enhancing NATO's Level 1 exploitation capability and ensuring it remains fit for purpose in a complex security landscape.

The WIT Trainer Developer Course: Preparing tomorrow's WIT instructors

Hosted from 1–5 December 2025 at the C-IED Centre of Excellence, the WIT TDC brought together 15 trainees from 9 nations, demonstrating the strong multinational commitment to strengthening WIT capabilities. As the Executing Agent of the WIT Training VNCF 2024–25 Agreement, the course focused on educating WIT Course Directors and Senior Instructors in the complete WIT Course Development Process. Throughout the week, significant effort was dedicated to enabling trainees to design, organize and deliver their own WIT courses.

The curriculum placed strong emphasis on developing a comprehensive understanding of NATO's minimum standards and national requirements for WIT training, while guiding participants through key principles of course design, scenario development and resource management.

The course's programme also highlighted emerging technological enablers, such as advanced 3D modelling tools and JDEAL capabilities, that enhance the effectiveness and accuracy of WIT activities. Through-

out the course, participants benefited from a rich exchange of knowledge and best practices, drawing on the diverse operational experience represented across the trainee group.

The WIT Review Workshop: Shaping the future of NATO WIT training

From 19–23 January 2026, the Spanish Armed Forces International Demining Centre (IDC) hosted the NATO WIT Review Workshop in Hoyo de Manzanares, Madrid. Eleven experienced participants from seven nations and the NATO Maritime Interdiction Operational Training Centre (NMIOTC) convened to systematically update the WIT course construct in accordance with the VNCF WIT Training Project 2026–27 Agreement.

For the participating nations, this workshop materialized an excellent opportunity to assess, synchronize, modify and update the WIT course content, in order to adhere to the latest standards, operational environments and technological solutions applied. The WS specifically focused on theory and practice in the current course construct, updating lectures and scenarios to better reflect the changing security environment facing NATO, updating and training forensics and WIT photography techniques to improve instructors' technical knowledge.

"*The strength of the WIT community lies in our ability to learn, adapt and improve together. This workshop is not just a review of what we have done, but a step forward in what we can achieve. Every insight shared here contributes to safer forces and stronger cooperation across the Alliance.*" — Rui Cordeiro, WIT Course Director

A clear direction for the future

Both the WIT TDC and the WIT Review Workshop demonstrated the synergy between training delivery and training development. The December course produced insights directly feeding the January workshop, while the workshop's outcomes will influence forthcoming course iterations beginning with WIT 26.1 in Romania.

Taken together, these events highlight several key themes: the TDC strengthened the instructor pipeline, while the Review Workshop modernized course content, instructional methods, equipment standards and training scenarios.

The C-IED COE remains fully committed to supporting the Alliance and Partner Nations in their capability building journey. Through dynamic training development, robust collaboration and an emphasis on innovation, the Centre ensures the WIT community remains prepared to meet emerging challenges and contribute decisively to NATO's broader C-IED and intelligence efforts.

For more information and registration procedures, visit *www.ciedcoe.org*

NATO C-IED COE support to operational and tactical exercises in a changing security environment

The contemporary security environment has forced NATO to rethink how the Alliance trains, plans and prepares for large-scale operations. Russia's full-scale invasion of Ukraine has demonstrated that modern warfare is characterised by a persistent hybrid activity, contested logistics, massed fires and an extensive use of unmanned systems, all of which present a complicated threat environment. In this context, the NATO-accredited Counter-Improvised Explosive Device Centre of Excellence (C-IED COE) has a challenging task in supporting NATO exercises at both the tactical and operational levels.

Over the last several years, the Centre has contributed to a growing number of NATO exercises, including exercises connected to the STEADFAST series as well as multinational activities such as Northern Challenge and Ardent Defender, spanning from the operational level to the low tactical level. Its support has increasingly focused on integrating C-IED considerations into operational planning, multi-domain operations, force protection, sustainment and rear-area security.

The operational environment observed in Ukraine has forced the C-IED discipline to face a reality far beyond the traditional counterinsurgency context. Improvised explosive devices, explosive hazards, remotely delivered mines, booby traps and unexploded ordnance are now encountered in high-intensity warfare alongside conventional military operations. Furthermore, both state and non-state actors have demonstrated an increasing ability to combine explosive threats with cyber operations, information activities, electronic warfare and unmanned aerial systems often used in combination with explosive payloads.

Exercises such as STEADFAST DUEL and STEADFAST DAGGER illustrate NATO's shift towards large-scale collective defence and multi-domain deterrence without losing the focus on the southern flank. STEADFAST DUEL is one of NATO's principal operational-level command post exercises designed to validate regional defence plans, command and control arrangements, and Alliance interoperability under Article 5 conditions. Similarly, STEADFAST DAGGER has focused on preparing the Allied Reaction Force for rapid deployment, crisis response and multi-domain operations in complex operational environments.

Within these exercises, the C-IED COE focuses on supporting scenario development, exercise control structures and training audiences with subject matter expertise linked to explosive threats and hybrid warfare. The support provided by the Centre typically includes integration of C-IED injects into operational scenarios, analysis of adversary networks, support to force protection planning and incorporation of explosive hazard considerations into sustainment and manoeuvre planning. This is particularly important in exercises simulating large-scale reinforcement operations across Europe, where lines of communication, ports, rail infrastructure, logistics hubs and staging areas remain vulnerable to sabotage, drones, mines and hybrid attacks.

One of the clearest lessons from Ukraine is that rear areas can no longer be considered secure. Operational support areas are now routinely targeted through long-range fires, loitering munitions, sabotage teams and improvised explosive attacks. As a result, NATO exercises increasingly train headquarters and subordinate units to operate in a degraded environment characterised by contested logistics and persistent disruption.

The renewed emphasis on operational-level exercises also reflects NATO's broader transformation after 2022. During the post-Cold War era, many NATO exercises focused on expeditionary crisis management operations outside NATO territory. However, recent

exercises have shifted toward collective defence, large-scale reinforcement and regional defence planning. This shift has also influenced the planning cycle for exercises. NATO operational-level exercises are increasingly designed as part of a continuous readiness cycle linked to regional defence plans, force model requirements and operational deterrence objectives. Rather than isolated training events, exercises are now connected to long-term capability development, lessons learned processes and Alliance-wide adaptation efforts.

The C-IED COE plays an important role within this cycle by feeding operational observations, lessons identified and doctrinal recommendations back into NATO's warfare development process. Lessons from Ukraine regarding explosive hazard management, protection of critical infrastructure and integration of unmanned systems into explosive threat environments are continuously shaping scenario development and exercise objectives.

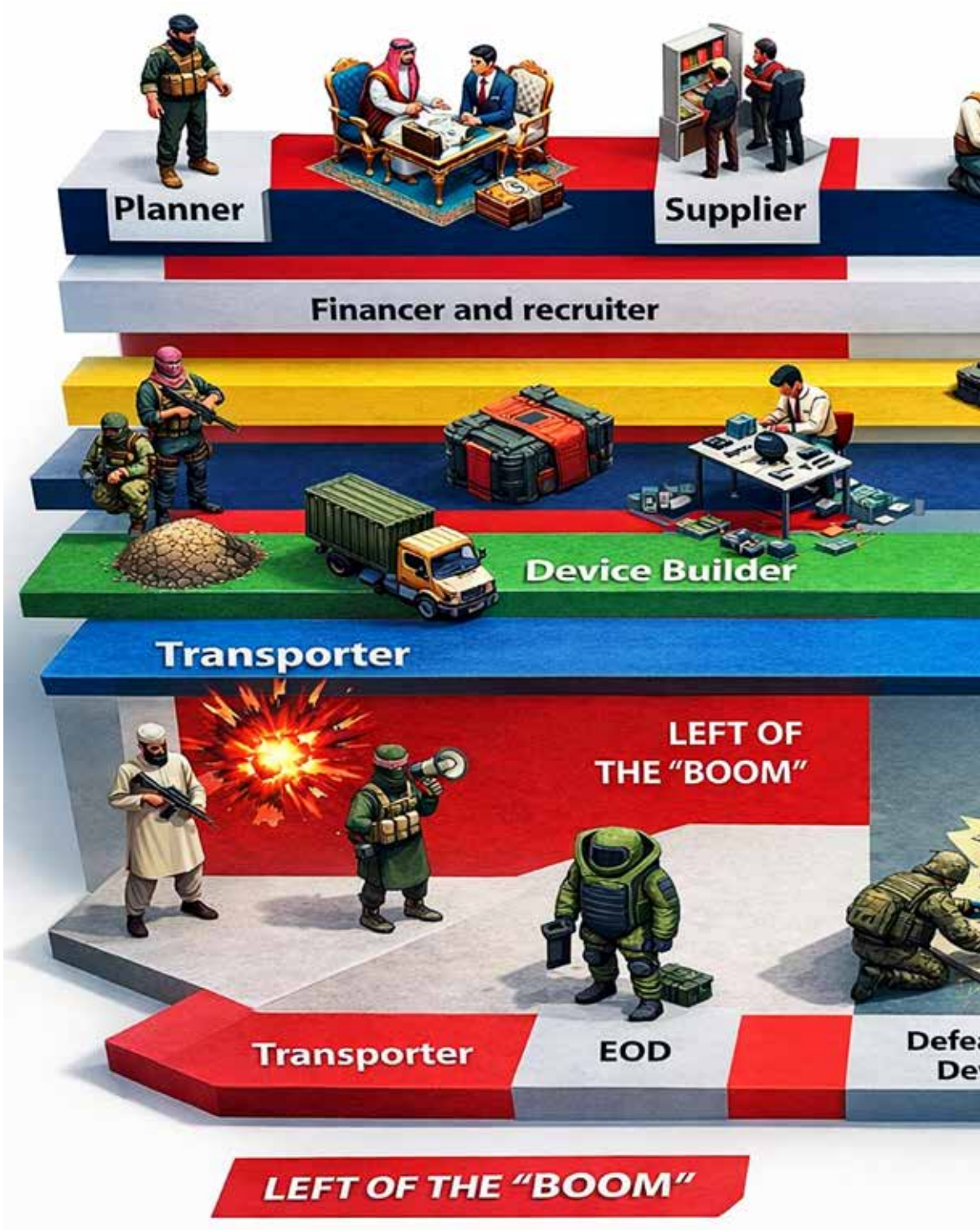
Another notable development is the increased integration of hybrid warfare dimensions into operational exercises. Modern scenarios now routinely include cyber disruption, disinformation campaigns, attacks on civilian infrastructure, GPS jamming and covert sabotage alongside conventional military operations. In this environment, the distinction between rear area security, force protection, counter-sabotage and C-IED operations becomes increasingly blurred.

Exercises such as the STEADFAST series have therefore become valuable opportunities to test how NATO forces coordinate across tactical and operational levels in a realistic threat environment. The inclusion of C-IED expertise within these exercises contributes to greater realism and it supports commanders in understanding how improvised threats influence tempo, freedom of manoeuvre, sustainment and operational resilience.

The operational lessons emerging from Ukraine also underline the importance of adaptability. Ukrainian battlefields have demonstrated rapid innovation cycles where new threats emerge quickly and tactical solutions evolve continuously. Consequently, the role of Centres of Excellence, including the NATO-accredited C-IED COE, has become increasingly important not only as providers of specialist knowledge but also as contributors to NATO's wider operational adaptation. Their participation in operational and tactical exercises ensures that lessons identified from current conflicts are translated into practical training, planning methodologies and operational procedures.

In many respects, NATO's current exercise programme reflects a return to collective defence, combined with a modern understanding of hybrid and multi-domain warfare. The operational environment is more contested, technologically dynamic and unpredictable than at any point since the Cold War. In this environment, explosive threats remain a central challenge and the C-IED COE will continue to play its role in helping the Alliance prepare for future

THE C-IED COE IS FOCUSED ON REDUCING CAPABILITIES OF HUMAN NETWORKS TO PREVENT THE "BOOM". THAT IS WHY WE WORK ON THE "LEFT OF THE IED SYSTEMS"



VISIT: ciedcoe.org

C-IED: WE ARE ON THE LEFT OF THE "BOOM"

ADDING C-IED AND TE PERSPECTIVE

CONFERENCES, SEMINARS AND WORKING GROUPS

Combined Annual Discipline Conference 2026

Counter-IED is one of the disciplines recognises by NATO as essential capabilities for the Alliance. Led by the Discipline Head and supported by the Requirement Authority, the second Combined Annual Discipline Conference, hosted at the Military Engineering Centre of Excellence (MilEng COE) in Ingolstadt, brought together NATO Command and Force Structure experts in the field of Energy Security, C-IED and Military Engineering.

As a part of the Global Programming cycle, the Community of Interest was informed by the Discipline Head about the status of Individual and Collective Training in C-IED.

Taking the given requirements of the discipline into consideration, the subject matter experts talked about possible changes due to the current global situation. The evaluation provided by the C-IED COE experts set another base for good discussions among the community of interest.

The Discipline Alignment Plan is the key outcome of this valuable conference for the training community. This document serves as a basis to align the Discipline according to individual and collective training needs. It will be published through the POC at ACT by September 2026.

C-IED COE hosts NATO Technical Exploitation, Battlefield Evidence and Biometrics meetings

A NATO hub for three connected communities

From 27 to 30 April 2026, the Counter-Improvised Explosive Devices Centre of Excellence (C-IED COE) hosted, at its facilities in Hoyo de Manzanares, Madrid, a series of NATO in-person meetings focused on Technical Exploitation, Battlefield Evidence and Biometrics.

The C-IED COE acted as host entity and provided organizational support to the meetings, conducted in support of NATO Headquarters International Staff, responsible for their convening. Over four intensive days, the Centre became a temporary NATO hub for three closely connected specialized communities, bringing together national representatives, NATO Bodies and NATO-accredited Centres of Excellence.

The event gathered approximately 85 participants from 19 NATO nationalities. Attendees represented Allied nations and NATO structures and entities, including NATO HQ, SHAPE, NCIA, SOFCOM, JFC Naples, JFC Brunssum and NATO MND-N. NATO-accredited Centres of Excellence also participated, including those focused on C-IED, HUMINT, Stability Policing and Military Police.

The programme included five meetings in four days: the NATO Technical Exploitation Group (NTEG) Plenary, the NATO Battlefield Evidence Working Group (NBEWG) Plenary, the NTEG Martial Vision Subgroup, the NBEWG Data Tiger Team and the NATO Biometrics Programme Coordination Group (NBPCG) Plenary. This concentration of meetings reinforced mutual situational awareness and cooperation among communities working on different aspects of the same operational problem.

Purpose of the Working Groups

The NATO Technical Exploitation Group provided the main forum for Allied nations and NATO Bodies to discuss the development, implementation and interoperability of Technical Exploitation within NATO. Its work addressed policy implementation, doctrine engagement, reporting standards, exercises, experimentation and information sharing. The NTEG Martial Vision Subgroup complemented this effort through focused work on TE processes, Allied Drone Exploitation and Information Sharing Reachback, support to the NATO Command Structure, major exercises and relevant NATO publications.

The NATO Battlefield Evidence Working Group provided the framework for Allied discussion on the implementation and further development of Battlefield Evidence within NATO. Its plenary addressed the implementation of the Military Committee Battlefield Evidence Policy, NATO policy updates, BE-related training efforts and the future programme of work. The NBEWG Data Tiger Team focused on Battlefield Evidence data management, including a draft NATO International Staff assessment on a NATO-owned communications and information system for Battlefield Evidence.

The NATO Biometrics Programme Coordination Group completed the sequence of meetings on 30 April. Its role was to coordinate NATO's biometrics-related work, aligning identity-focused capabilities, requirements, training, standardisation and future activities with operational needs. In this event, the NBPCG also linked with the Technical Exploitation and Battlefield Evidence communities, especially where biometric data, identity intelligence and human network analysis

support a common operational picture, interoperability and information sharing across NATO.

Across all meetings, common themes emerged: policy implementation, doctrine development, standardisation, education and training, data management, exercises, experimentation, information sharing and interoperability. Technical Exploitation, Battlefield Evidence and Biometrics each provide specific contributions, but their value increases when they are connected through common procedures, shared standards and coherent information flows.

Icebreaker and informal Table-Top exercise

A relevant element of the week was the joint icebreaker and informal Table-Top Exercise. Designed for all participants, it combined networking with a structured team-based role-playing TTX.

The activity placed participants in a simulated but realistic joint force operating environment, framed within a multi-domain deterrence and defence scenario. It featured tactical through strategic play involving Technical Exploitation, Battlefield Evidence and Biometrics. Its purpose was to promote interaction, stimulate joint problem solving and build a shared understanding of the challenges and benefits of a robust NATO TE, BE and Biometrics framework.

The C-IED COE as a natural platform for TE and BE

The meetings highlighted the role that the C-IED COE can play in the further development of these specialised areas, particularly Technical Exploitation and Battlefield Evidence.

The Centre already works at the point where the device, the network and the operational environment meet. The C-IED approach supports understanding, anticipation and disruption of the wider system that enables the threat, including human networks, supply chains, technical signatures, TTPs, forensic outputs, identity-related information and operational lessons.

The C-IED COE is well placed to contribute to this effort because of its multinational composition, connection with NATO structures, training experience, support to exercises, and technical and operational expertise. It can serve as a forum where TE and BE doctrine, training, experimentation, lessons learned and operational requirements are brought together.

The April meetings therefore reinforced an important message: the C-IED COE is not only a venue. It is a relevant Allied platform for connecting communities that must work together.

Conclusions

The 27–30 April meetings at the C-IED COE provided a concentrated opportunity for NATO nations, NATO Bodies and specialised Centres of Excellence to address Technical Exploitation, Battlefield Evidence and Biometrics in a coordinated manner.

The event demonstrated the operational value of bringing these communities together. It supported mutual situational awareness, strengthened personal and institutional links, and enabled discussion on policy, doctrine, training, exercises, data, interoperability and future requirements.

As NATO continues to adapt to multi-domain operations and evolving threats, TE, BE and Biometrics will remain essential to understanding adversary networks, supporting commanders, preserving evidence, enabling accountability and improving Allied interoperability. The C-IED COE, by hosting these meetings and supporting their interaction, confirmed its value as a trusted NATO hub for expertise, coordination and future development in these critical specialised areas.

Soldier in the Spotlight

Lt. Cdr. (TUR N), Murat Aydogmus

LtCdr Murat Aydogmus, from the Turkish Navy, has already been in our Centre for 3 years. Before he leaves to occupy his next position, we have asked him several questions to find out more about his educational path, his professional career and how he ended up in the fight against IED.

When and how did you get interested in the Armed Forces and, particularly, in the Navy?

I remember how much I admired and looked up to the people in uniform when I was in middle school. I took a major step toward realizing this dream after being successful on the exams and enrolling in a military school at the age of 15. Military life is a profession with clearly defined boundaries and requires strong discipline. Additionally, the Navy is a way of life with its own traditions and customs. From the very first day I put on the uniform, I felt that this lifestyle suited me perfectly and I still feel the same way today.

Were your first postings related to the fight against IEDs?

Throughout my career, I have worked in technical roles and positions and, due to my specialization, I continue to work in a technical field here as well. I can say that I was first introduced to IEDs at this centre. I consider this experience as part of all the technical roles I have worked on so far.

What kind of training did you follow in this area?

I hold both a bachelor's and a master's degree in Electronics Engineering. In addition, my doctoral studies are also focused on Electronics Engineering. Therefore, appart from my academic background, I can also include the courses I have taken in this field. These courses are more specialized and practice-oriented, focusing on specific topics.

How would you describe your experience at the C-IED COE, living in Spain, but in an international environment?

It was definitely a very good experience for me. First of all, working in an international environment and having the opportunity to experience different working and social life cultures were both unique and valuable. It helped me broaden my perspective professionally and personally.

I can also say that life in Spain was very positive for us. At the beginning, a new environment, a new school and new faces could have made the process quite challenging for my family and child. However, fortunately, everything went very smoothly. It did not take long for us to adapt and start enjoying life here. In that sense, we consider ourselves quite lucky.

Which have been your main assignments at the C-IED COE?

Throughout these 3 years at the C-IED COE, I have contributed to the courses and exercises as an SME. Also, being part of the organization team for the Centre´s diamond events was really important for my personal development as well as understanding how multinational events are organized.

I believe you are working to get your PhD, could you tell us more about it?

As I mentioned, my PhD is in Electrical and Electronics Engineering and is a continuation of my master's studies. My research focuses on underwater object detection using state-of-the-art deep learning models for autonomous decision-making in unmanned systems. I believe this is a highly promising and exciting research field.

Through my studies, I have improved my skills in artificial intelligence, computer vision and deep learning applications. I am also gaining experience in developing reliable and efficient systems for real-world underwater environments, where challenges such as low visibility and limited data make the problem more complex.

What professional challenges do you pose yourself for the future?

First of all, in every position and responsibility assigned to me, I will do my best to represent my role and organization in the most professional and effective way. In addition, I plan to continue improving myself academically and pursue further academic studies alongside my professional career.

UPCOMING EVENTS 2026

C-IED COE main activities 2nd semester 2026

This is the C-IED COE planning for 2026 with regard to courses approved by the Steering Committee on 19 November 2025. Below dates may change due to unforeseen reasons. No rights can be inferred according to this schedule.

NATO Weapons Intelligence Team Course (WIT) 26.2
7-Sep

Document & Media Exploitation Course (DOMEX) 26.2
TBC-Sep

Alternate Threat Scenario (ATS)
15-Sep

Lessons Learned Workshop (LLWS)
14-Oct

Analyst Notebook User Course (ANUC) 26.3
19-Oct

C-IED Staff Officer Course (CSOC) 26.3
26-Oct

AtN Operational Course (ATNOC) 26.2
9-Nov

WIT Training Developer Course 26
30-Nov

Steering Committee 2026
01-Dec

Latest C-IED COE reports

The Centre continues to strengthen its role as a knowledge hub through the production of periodic analytical reports that are regularly distributed to the Community of Interest. These reports—ranging from threat assessments and doctrinal updates to technology reviews and operational insights—provide timely, relevant and actionable information to decision-makers and practitioners across the Alliance.

By consolidating expert analysis from all branches of the COE and transforming it into clear, accessible products, the Centre ensures that its expertise directly contributes to improved situational awareness and better-informed planning.

Here is a sample of the reports distributed since the last edition of the Chessboard magazine:

- **Evolution of the Use of Explosive-Laden Drones by Terrorist Groups and Threat Forecast**
- **UAS Threat Foresee Report**
- **Evolution of Daesh-Somalia TTPs and their links to the HOUTHI**
- **Outputs and outcomes from the first official communication from the DAESH leadership in 2025/2026**
- **Update – Explosive-related Threats from Pro-Iranian Militias in Lebanon**
- **UN Working Group on the Use of Mercenaries**
- **Autonomous Swarm Attack Scenarios using UAS**
- **African Drone Threat Expansion and Criminal Convergence**

These reports have been sent to our e-mail distribution list and are also available in the restricted area of the public website: www.ciedcoe.org.

If you wish to receive the reports issued by the C-IED COE, please contact: info@ciedcoe.org

Become a Partner of Chessboard

Showcase Your Innovation. Support the Mission.

Chessboard, the official publication of the C-IED COE, invites private companies and industry leaders in the C-IED sector to join us as sponsors of our high-quality printed edition.

By advertising your products or services in Chessboard, your company will:

- **Gain visibility among NATO, partner nations and key decision-makers. The electronic version of the magazine is shared with the 450 members of our distribution list (NATO, EU, UN, Law Enforcement and Intelligence agencies, Academia, etc).**
- **Reach a curated, multinational audience of experts in military operations, law enforcement, technical exploitation and homeland security.**
- **Demonstrate your commitment to innovation, safety and international cooperation in the fight against IED threats.**

In return, your sponsorship helps us:

- **Deliver a professionally printed, full-colour edition of the magazine.**
- **Distribute it free of charge at major events, such as:**

  - CIEDAC Annual Conference.
  - C-IED COE courses and seminars.
  - Workshops and collaborative forums.

Your technology deserves to be seen. Your brand deserves to be trusted.

Join Chessboard as a sponsor and position your company at the forefront of the global C-IED effort.

Contact us: chessboard@ciedcoe.org

C-IED COE LODGE

The Counter-Improvised Explosives Devices, Centre of Excellence, has in its facilities a lodge with 60 single/double rooms and common areas, with living room and dining room, outdoor garden, terraces and self-service laundry. **The main goal is to give accommodation to the people attending the COE courses and events.**

All rooms have television connected to satellite, WIFI, refrigerator, study area and own bathroom with shower, as well as provision of sheets, towels and amenities.

The lodge is located inside of "Academia de Ingenieros" barracks, 1.5 km far from the COE main building, inside the Regional Park of the Cuenca Alta del Manzanares, in the municipality of Hoyo de Manzanares, at a distance of 35 km from Madrid Capital City.

billeting@ciedcoe.org

Enabling NATO's Multi-Domain Future

The C-IED Centre of Excellence is committed to becoming the global hub for C-IED knowledge, integrating military expertise with the contributions of law enforcement, intelligence agencies, academia, and industry.

As NATO evolves towards Multi-Domain Operations, our mission is to ensure that C-IED capabilities deliver decisive effects across the physical, virtual, and cognitive dimension—supporting transformation, interoperability, and operational success across the Alliance.

+34 91 856 10 48
info@ciedcoe.org
www.ciedcoe.org