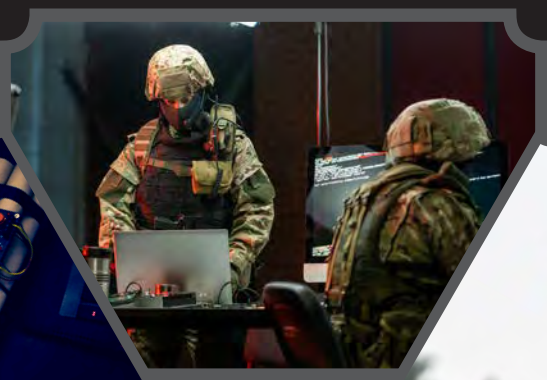
YOU ARE IN THE C-IED

CHESSBOARD

INSIGHTS FROM NATO's C-IED EXPERTS

DEC 2025 | ISSUE 04

Prepare the Force

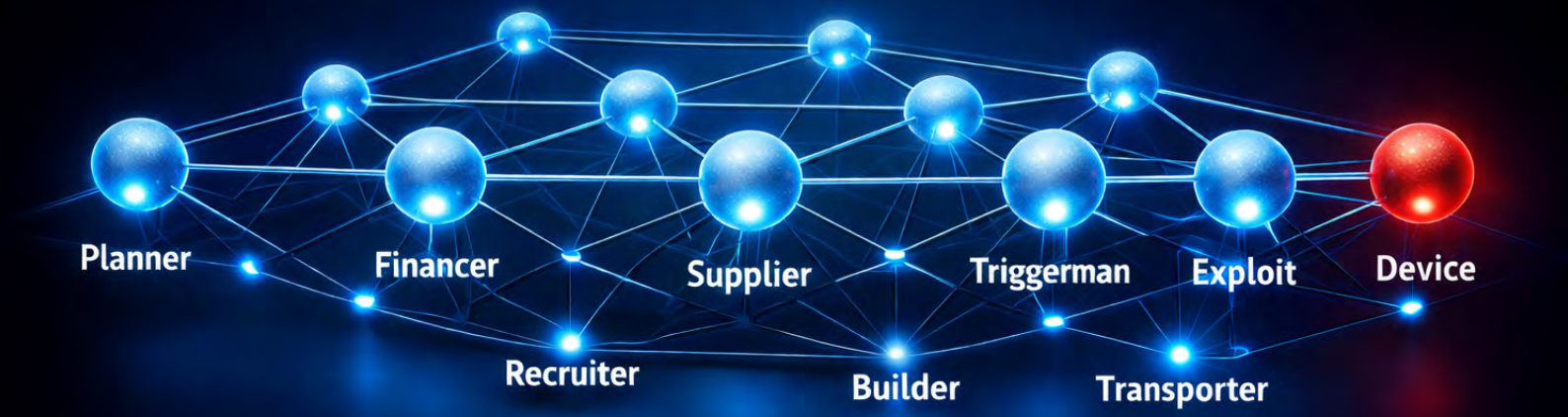


Attack the Networks

Defeat the Device

C-IED COE

15 Years fighting the IED Systems



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)
1stLT (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 Mustafa Çelik (TUR A)
LTC José Manuel Rufas Símón (ESP A)
LTC Mathias Döpping (DEU A)
LTC Carlos García de Paredes Ucero (ESP MC)
LTC Félix Ortega Medina (ESP A)
LTC Fernando Martel Muñoz-Cobo (ESP A)
LTC José Manuel Veiga Torres (ESP A)
LTC Luis Bermejo Pérez (ESP A)
LTC Juan Carlos Lage Carreira (ESP MC)
MAJ Juan Manuel Mancilla López (ESP MC)
MAJ Alberto Brunhöfer García (ESP A)
MAJ Georgios Krikelis (GRC A)
MSGT David Herráiz López (ESP A)
SFC Miguel Perez (USA A)

DISCLAIMER

This publication is a product of the NATO C-IED Centre of Excellence. It does not necessarily reflect the policy or the opinion of NATO. The Centre may not be held responsible for any loss or harm arising from the use of the information contained in this publication and it is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for nonprofit and non-commercial purpose, provided that copies bear a full citation.

Unless other identified, the photographs and sketches shown in this document are the sole property of the C-IED COE and the presentation copyrights owners have authorized its publication.

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 members of the C-IED Community of Interest,

It is with great pleasure that I introduce this issue of our magazine, my first as Director of the C-IED Centre of Excellence. This edition holds special significance as we commemorate the 15th anniversary of the Centre's accreditation, a milestone that reflects years of dedication to countering the ever-evolving IED threat. It was an honor to mark this occasion with a celebration presided over by the Spanish Chief of the Joint Staff, Lieutenant General, José Antonio Herrera Llamas, and to welcome the members of the Steering Committee and diplomatic representatives from all our Sponsoring Nations.

Within these pages, you will find a concise journey through the Centre's history, highlighting key achievements and contributions to NATO, its partners and the wider international community. We also delve into the challenging future that lies ahead and explore potential paths for the C-IED COE to evolve and adapt to the current strategic landscape, ensuring our continued relevance and effectiveness.

Furthermore, we bring you the highlights from our recent C-IED event in Málaga, CIEDAC 2025. With almost 200 attendees representing military, law enforcement, academia and defense industry partners from across the globe, the event was a resounding success. It was a valuable opportunity to foster dialogue, share knowledge and strengthen the bonds within our community. We are looking forward to hosting the next iteration of this Annual Conference in Valencia, in June 2026.

Finally, I sincerely hope that the featured articles within this issue spark your interest, encourage discussion and contribute to our collective efforts in countering improvised explosive systems. Thank you for your continued trust and partnership.

Sincerely,

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

Adapting to the Future: Possible Paths for the Evolution of the C-IED COE

Since its accreditation in 2010, the C-IED COE has been a unique instrument in NATO's toolbox. Created with the mission of supporting the Alliance, its partners, and the international community in the fight against improvised explosive devices and the threat networks that employ them, the Centre has delivered tangible results for more than fifteen years. By supporting operations, it has helped reduce casualties, protect freedom of movement and strengthen multinational interoperability in asymmetric environments.

Fifteen years on, the security landscape in which the C-IED COE operates is changing at an accelerated pace. The type of threat, once centered almost exclusively on land-based IEDs, has now evolved into new, more complex manifestations across the physical domains: unmanned systems carrying explosives, improvised weapon systems built with commercial components, or hybrid networks blending criminal, insurgent and state-backed actors.

Moreover, the operational environment is no longer restricted to physical battlefields: it now encompasses the cyber domain as well, considering also the cognitive warfare as one of the most significant factors, where influence, disinformation and disruptive technologies also play decisive roles.

In this context, the Centre is confronted with a crucial question: how should it adapt to remain relevant and effective in the future strategic environment? The answer is not a single path, but rather a set of possibilities currently under reflection. No final decision has been made, but discussions within the Centre, with Allied Command Transformation (ACT), and among Sponsoring Nations are pointing toward several avenues of adaptation.

Structural Adaptation: From Three Pillars to Four

The current three-pillar structure of the C-IED Centre of Excellence does not align with the standardized framework of NATO's Centre of Excellence (COE) programme, as defined by Allied Command Transformation (ACT). This misalignment limits the Centre's flexibility and resilience, reducing its ability to effectively contribute to Warfare Development and meet the evolving requirements of the Alliance in a complex, multi-domain operational environment.

In an era defined by rapid change and emerging threats, NATO COEs must continuously evolve to remain relevant and mission effective. To serve the Alliance optimally, COEs are expected to deliver recognized expertise and operational value within clearly defined subject matter areas, structured around the four foundational pillars of NATO's COE program: Education, Training, Exercises and Evaluation; Analysis and Lessons Learned; Concept Development and Experimentation; and Doctrine Development and Standardization.

We need to remove the "Stigma from the Past", where C-IED capabilities were often narrowly perceived, both within the Alliance and beyond, as tools primarily designed to counter Terrorism, Insurgencies or Violent Extremist Organizations. This legacy view overlooks the broader applicability of C-IED in high-intensity, peer-conflict scenarios, particularly within Multi-Domain Operations (MDO) under Article 5 conditions.

By realigning the COE's organizational structure with current NATO guidance and MDO-focused direction, the Centre will position itself for broader relevance and increased acceptance across the Alliance. This transformation will enable more effective support to exercises, doctrine and standardization efforts, concept and capability development, and education and training initiatives, ensuring that C-IED remains a vital enabler in future warfare.

Expanding the Mission: Beyond Counter-IED

With the new structure established, a comprehensive assessment will be undertaken to ensure the C-IED COE remains aligned with NATO's evolving priorities and future operational requirements. Identifying potential enhancements to the Centre's mission and expertise, including the integration or expansion of other activities, such as Technical Exploitation (TE), Battlefield Evidence (BE) and Emerging Threats would strengthen the Centre's relevance across the broader spectrum of C-IED operations.

Modern conflicts are demonstrating that the technical exploitation of materials, the analysis of battlefield evidence and the integration of these findings into operational and strategic decision-making are as critical as the neutralization of the devices themselves. The Centre could become NATO's reference institution for C-IED, TE and BE disciplines.

A New Identity?

If these structural and mission-related adaptations are pursued, even the name of the Centre should evolve. One of the ideas already discussed in the C-IED community of interest is the possibility of becoming the Counter-Improvised Explosive Systems and Battlefield Forensics Centre of Excellence (C-IES&BF COE).

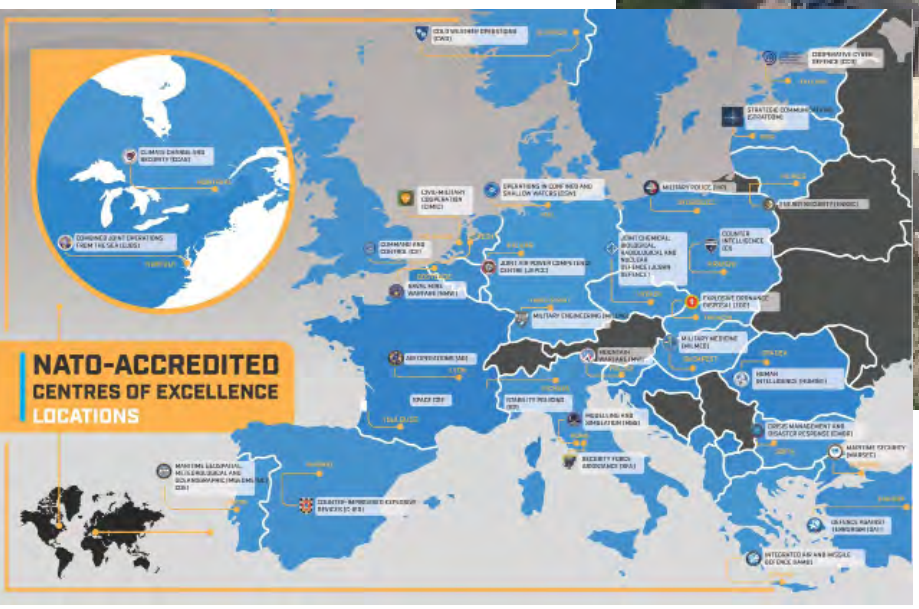
Such a change would better reflect the broader spectrum of threats and the expanded skill set encompassed within the Centre. However, it is important to stress that this remains a proposal under study, not a decision. This identity shift is essential to ensure the COE remains future-ready, interoperable and aligned with NATO's evolving warfare development agenda.

Looking Ahead

While the future will undoubtedly present new challenges, the C-IED COE stands resolute in its commitment to readiness. Its deep expertise in human network analysis, targeting, intelligence fusion and interagency cooperation forms a robust foundation for any path forward.

Whether through alignment with NATO's four-pillar framework, an expanded mission encompassing TE and BE, or the evolution of its name and identity, the Centre remains agile and forward-looking, poised to maintain its relevance and reinforce Allied and Partner security in an ever-changing threat landscape.

This anniversary marks not only a celebration of the Centre's fifteen years of meaningful impact, but also a pivotal moment to consider the pathways for its future evolution. Whatever direction is ultimately chosen, one guiding principle will remain unwavering: to ensure that the C-IED COE continues to serve NATO, its member nations and partners as a trusted nexus of expertise, innovation and collaboration in countering ever-evolving threats.



WHAT IS A CENTRE OF EXCELLENCE (COE)?

A 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 (ALL)
- Doctrine development and standardization (DDS)
- Concept development and experimentation (CDE)

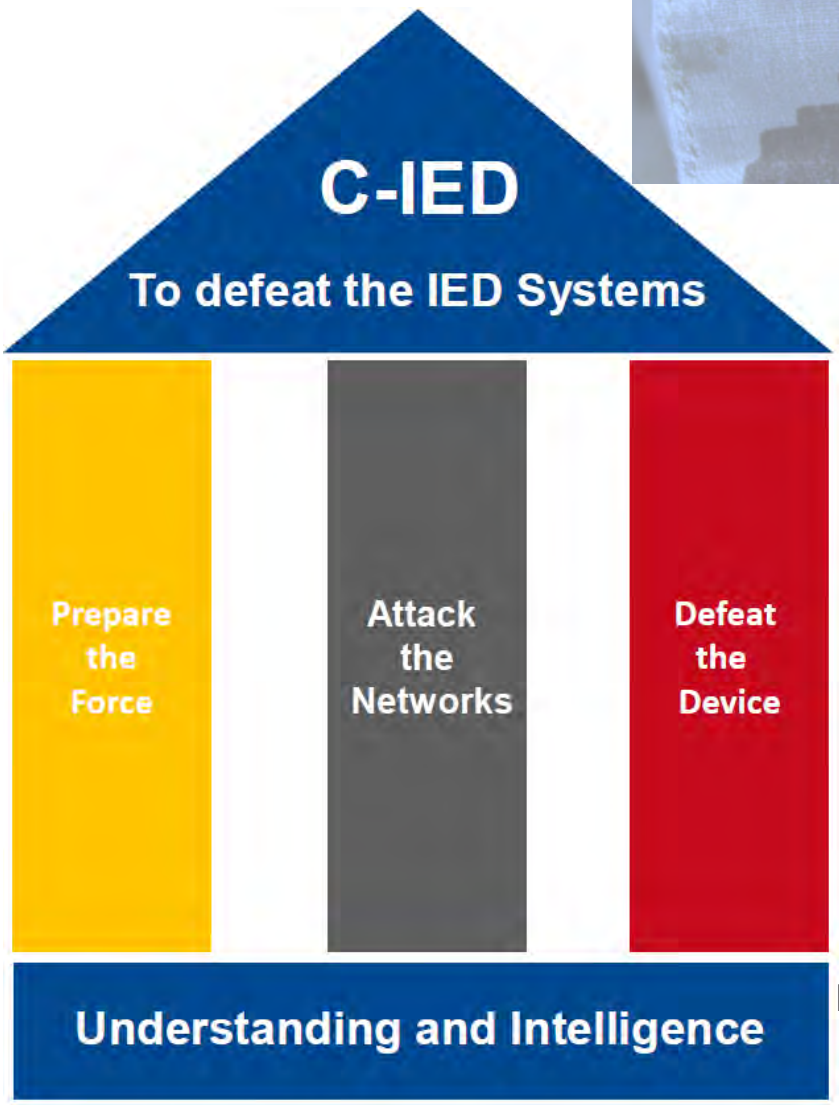
MORE INFO
act.nato.int/about/centres-of-excellence

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 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 insurgents.



ATTACK THE NETWORKS IS THE MAIN DOCTRINAL PILLAR OF C-IED...

... FOR THIS REASON, THE ACTIVITIES ARE GEARED TOWARDS INTEL'S ACTIVITIES AND OPERATIONS

C-IED COE HIGHLIGHTS

Steering Committee Meeting at the C-IED Centre of Excellence

The Steering Committee of the Counter-Improvised Explosive Devices Centre of Excellence (C-IED COE) convened on 18–19 November at the Centre's facilities in Hoyo de Manzanares, Spain.

The chairperson was Colonel Fernando Cano Artero, representing the Spanish Joint Staff. He opened the session by welcoming the participants and underlining the importance of collective efforts to counter the IED threat within NATO and Partner Nations.

The meeting gathered national representatives from the 12 Sponsoring Nations, with the exception of Türkiye, which joined via videoconference, and Canada, still participating as an observer.

Over the two-day session, the Committee reviewed the activities carried out in 2025 and approved the Programme of Work (PoW) for 2026. In addition, the Financial Statement for 2024 was endorsed, the status of the 2025 budget was examined, and the estimated expenditure for 2026 was approved.

A major outcome of the meeting was the endorsement of the Centre's strategic framework for the coming years, which includes five Lines of Effort aimed at keeping the Centre relevant, fostering modernization, enhancing education and training, strengthening external collaboration, and improving internal cohesion.

In addition, the Steering Committee acknowledged the Director's remarks on the evolving threat landscape and agreed on the importance of adapting the Centre to remain effective and relevant. To address this, the Director outlined a revitalization concept that will guide the Centre's transformation over the next two years.

This plan introduces structural adjustments to improve efficiency, proposes an evolution of the Centre's mission to incorporate emerging capabilities, and anticipates changes that reflect its future orientation. The detailed roadmap will be refined in the coming months and submitted for formal approval by the Sponsoring Nations.

By endorsing these strategic elements, the Steering Committee reaffirmed its commitment to maintaining the C-IED COE as a leading institution in the fight against Improvised Explosive Devices, ensuring alignment with NATO priorities and operational needs.

Celebrating 15 Years of Excellence: The C-IED COE 15th Anniversary Ceremony

On 20 November 2025, the C-IED COE marked its 15th Anniversary with a ceremony held at its premises in Hoyo de Manzanares (Madrid, Spain). The event was presided over by Lieutenant General José Antonio Herrera Llamas, Chief of the Spanish Joint Staff, whose presence highlighted the strategic importance of the Centre within NATO's security and transformation landscape.

The ceremony gathered military and civilian authorities, members of the diplomatic corps, Steering Committee national representatives and former COE directors. The day began in the flag esplanade, where guests were welcomed by COE staff and national Senior Representatives. After the arrival of the presiding authority, the Spanish military march

"Marcha de Infantes" was played before the formal opening remarks.

A particularly symbolic moment was the raising of the Canadian flag, marking Canada's accession as a future Sponsoring Nation of the Centre. Following the approval of its Note of Joining by all twelve current Sponsoring

Nations, this act represented Canada's long-standing cooperation with the COE and its growing commitment to NATO's counter-IED community. The flag was carried by WO Ian Foreman and raised by LtCol Steve Rau, Canadian representative to the Steering Committee.

After the flag-raising, all attendees moved to the Main Conference Room, where the ceremony continued with a presentation video highlighting the structure, missions and global activities of the Centre. The presiding authority delivered an address recognising the COE's contribution to the fight against IED systems and the continued relevance of the C-IED discipline in today's threat environment. The Director of the Centre followed with a speech reflecting on 15 years of progress, partnerships and operational impact.

One of the central moments of the ceremony was the presentation of the 15th Anniversary Book, a commemorative volume capturing

the evolution, achievements and future vision of the C-IED COE. Afterwards, ambassadors and flag officers visited the laboratories and classrooms, where they received briefings on the Centre's most recent projects.

The celebration concluded with a reception at the Noble Room of the Engineers' Academy, where the presiding authority offered an official toast. Far beyond a formal closing, the gathering became a moment of genuine social exchange and mutual understanding, bringing together Steering Committee members, diplomatic representatives, national authorities and COE

personnel in an atmosphere of camaraderie and shared purpose. Conversations flowed naturally—from professional insights to personal experiences—strengthening the human bonds that sustain multinational cooperation. The reception offered a valuable space to deepen relationships, foster trust and celebrate the collective effort behind the Centre's achievements over the past 15 years, while looking ahead with renewed unity to the challenges of an increasingly complex global security environment.

Fifteen years after its establishment, the C-IED COE stands as a reference within NATO—an institution shaped by multinational cooperation, operational experience and an enduring commitment to saving lives and strengthening collective defence. The anniversary ceremony not only celebrated its past achievements but also set the tone for its future role in supporting the Alliance.

MENPRO

GARANT protects

Boston Dynamics

eia®

PERSISTENT SYSTEMS

MENPRO SL

info@menpro.es - +34-915522161 – www.menpro.es

28521 Rivas Vaciamadrid – Madrid, Spain

Canada, the newest member of the C-IED COE

In a significant step for trans-Atlantic defense cooperation, Canada took another step towards formally becoming a Sponsoring Nation of the C-IED COE. This event was marked by the ceremonial raising of the Canadian national flag alongside those of the existing Sponsoring Nations, symbolizing Canada's full commitment to the Centre's mission and its integration into the multinational framework.

On 20 November 2025 at the C-IED COE, representatives of the Canadian government and military joined the Centre's Director and delegates from the Framework Nation, Spain, and the other Sponsoring Nations. After brief remarks, the Canadian flag was hoisted, to the accompaniment of the national anthem, while staff and visitors stood in respectful formation.

This moment underscored Canada's arrival as a full partner in the Centre's operations, a visible sign of solidarity with all those working to counter the improvised explosive devices threat.

Canada's sponsorship means it will have a say in the Steering Committee, contribute subject-matter experts, and help shape doctrine, training and lessons-learned in this important domain. It also visibly reinforces Canada's commitment to Allied security beyond pure troop deployments.

To become a Sponsoring Nation, Canada had to sign a Note of Joining to the Centre's Memorandum of Understanding (MoU), approved by all existing Sponsoring Nations. The updated version of the MoU including

Canada as a Sponsoring Nation is currently in the process of being signed by all Sponsoring Nations.

Canada formally requested to join the Centre as a Sponsoring Nation in 2021. During this phase, the Canadian Defense Attaché in Madrid visited the Centre with a delegation from the Canadian Embassy. At the same time, Canadian personnel began contributing on a voluntary basis to the Centre's staff.

The first member to assume a position at the C-IED COE was OR-8 Sebastien Guay, who arrived in August 2022 and spent 2 years in the Attack the Network branch. Canada's current member, OR-7 Ian Foreman has been posted to the Prepare the Force branch since August 2024.

Canada's accession as a Sponsoring Nation of the C-IED Centre of Excellence represents far more than an administrative milestone: it marks a strategic investment in Allied readiness and a visible reaffirmation of Ottawa's commitment to collective security.

With the raising of the Canadian flag at the Centre, Canada positions itself as an influential contributor to NATO's ongoing transformation efforts, elevating its profile within the multinational community of nations combating the evolving IED threat.

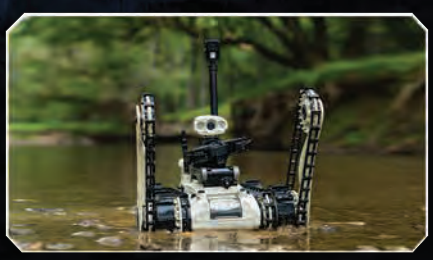
The benefits of this new partnership are both immediate and far-reaching. Canada's involvement strengthens its leadership role in counter-IED doctrine, training and capability development, placing Canadian expertise at the heart of some of NATO's most dynamic operational and conceptual advances. Canadian forces, instructors, and defense researchers will now gain enhanced interoperability through access to the Centre's multinational training environment, specialized knowledge base, and expanding network of European partners and intelligence actors.

In turn, Canada's participation enriches the COE's collective capacity to anticipate, adapt and respond to emerging IED challenges. As the threat continues to evolve across domains and theatres, Canada's sponsorship reinforces the Centre's mission and strengthens the Alliance's shared resilience.

PERSISTENT SYSTEMS

NETWORKING THE MARITIME ENVIRONMENT

Built to create powerful, secure networks anywhere, the MPU5 unites all your critical data sources in real time – enabling efficient decision-making in any clime or place.



www.persistentsystems.com

ENGAGE!

EVENTS

CIEDAC25 Málaga
A New Global Hub in the Fight Against IEDs

The first edition of the C-IED Annual Conference (CIEDAC25), held in Málaga, marked a decisive step forward for the international community dedicated to countering the threat posed by IEDs. Organized by the NATO-accredited C-IED COE, the conference consolidated more than fifteen years of workshops, interagency seminars, and technical meetings into a single, coherent, strategically oriented annual event.

The central theme — "Countering the IED System in Support of Multi-Domain Operations" — shaped every session. In an operational environment increasingly dominated by hybrid threats, the use of IEDs remains a decisive factor for both state and non-state actors. Multi-Domain Operations (MDO) require integrating intelligence, technical exploitation, influence activities, EOD capabilities, cyber and network analysis into a unified effort capable of anticipating, disrupting and neutralizing ever more complex threats.

Held at the Ilunion Málaga Hotel, CIEDAC25 combined keynote presentations, expert panels, technical sessions, technology demonstrations, and networking activities, including bilateral meetings, an industrial exhibition area and a cultural visit. The presence of high-level stakeholders — military leaders, security agencies, academic institutions and cutting-edge technology companies — underscored the COE's growing role as a doctrinal, educational and operational reference point.

The strength of the event lay in its diversity: NATO commands, Allied armed forces, European and North American police organizations, research

centers, universities and industry representatives all shared the same space. This mix — operational, academic and technological — allowed debate to evolve into concrete proposals for the future transformation of C-IED capabilities.

The event received additional backing from NATO's Counter-Terrorism Section within the Operations Division. Through NATO's Defence Against Terrorism Programme of Work, this section drives the development and deployment of advanced military capabilities and innovative operational concepts designed to safeguard Allied forces, territories and populations against terrorist and asymmetrical threats. Thanks to this vital support, the COE was able to deliver a truly world-class event, offering an exceptional experience for both attendees and exhibitors.

Evolving Threats: From DAESH to Adaptive Human Networks

Among the most impactful presentations was an analysis of emerging threat environments. Experts discussed the persistence of structures inspired by DAESH, as well as the rise of transnational criminal networks that blend low-cost technologies, decentralized structures, and outsourced processes. The evolution of chemical IEDs and the increasing availability of dual-use materials were also prominent topics.
The network-centric targeting approach — essential to the doctrinal pillar Attack the Networks (AtN) — featured heavily throughout the conference. Recent case studies were presented involving human network analysis, financial tracking, and data exploitation to identify key nodes within threat systems. Representatives from European police agencies emphasized the importance of the human sensor and civil-military cooperation in urban settings.

Technology and Technical Exploitation: From 3D Reconstruction to Forensic Laboratories

The Defeat the Device (DtD) pillar took center stage with demonstrations that covered:

- 3D reconstruction of post-blast scenes.
- Advances in chemical analysis methodologies.
- Technical Exploitation in maritime environments.
- Integration of deployable laboratories with national forensic capabilities.

Speakers highlighted the operational relevance of technically exploitable results across MDO scenarios: from feeding strategic intelligence to enabling legal action and supporting the development of tailored countermeasures.

Training, Education and Doctrine

The section dedicated to Prepare the Force (PtF) emphasized the need to incorporate the C-IED perspective into multi-level operational planning. Updates were presented on doctrinal integration, enhancements to NATO-accredited courses, and lessons identified from recent exercises.

A central point of consensus was the need — still pending in some nations — to view the C-IED approach as a strategic capability rather than purely a technical one. Integrating the C-IED mindset into standard planning processes, as well as its alignment with Digital Transformation and MDO initiatives, was repeatedly underscored.

Industry, Technology and a Growing Ecosystem

One of the most valuable aspects of CIEDAC25 was its technology exhibition. There, leading defense and security companies showcased solutions in fields such as:

- Sensors and UAS/Counter-UAS platforms.
- Technical Exploitation tools (forensic software, chemical analysis, digital evidence processing).
- IED neutralization systems.
- Simulators and training tools.
- Network analysis, AI and big-data capabilities.

Their involvement extended far beyond exhibition booths: many companies actively contributed to panels and discussions, bringing an industry-oriented, innovation-driven perspective into the operational debate. This exchange highlighted the increasing convergence between military requirements and the private sector's technological developments.

CIEDAC: The New Flagship of the C-IED COE

The conference reaffirmed the C-IED COE's leadership within NATO as a doctrine and knowledge hub, a multinational focal point, a driver of innovation and experimentation, and as a bridge between industry, armed forces and law enforcement.

CIEDAC25 Málaga was born with the ambition of becoming the reference conference in the C-IED domain and it succeeded from its very first edition. Its comprehensive approach, quality of speakers, industrial presence, thematic breadth and alignment with NATO's priorities in MDO and transformation have positioned it as an essential forum for all professionals involved in international security.

Established as the flagship event of the C-IED COE, CIEDAC is poised to continue growing in participation, influence and operational relevance in the years to come.

FEATURED ARTICLES

Comprehensive Technical Exploitation of Explosive-laden Drones

Nowadays, the threat dynamics from explosive-laden unmanned aircraft systems (UAS) are posing a trending topic with an associated growing demand of updated information, innovative solutions, and development of supportive tools to face the potential risks derived from the use of those flying weapons.

With regards to Technical Exploitation (TE), and from the perspective of Defeat the Device (DtD), there is a need to investigate explosive-laden drones as collected exploitable material (CEM) in support of the identification of technical trends, force protection (FP), explosive ordnance disposal (EOD), detection of associated IEDs, and mitigation of their effects, as well as for research & development (R&D) in the benefit of technological developments for physical protection.

From an Attack the Networks approach, the Technical Exploitation of explosive-laden drones is essential to anticipate the threats, identify adversary tactics, techniques & procedures (TTP), understand the capabilities of adversary human networks, study own potential vulnerabilities exploitable by opponents, track components and instructional sources, and support identity intelligence in benefit of human network engagement.

In most cases, the currently available training on technical exploitation of UAS is limited to commercial-off-the-shell (COTS) models and mainly focused on the application of digital media exploitation (MEDEX) and cellular phone exploitation (CELLEX) over them.
Under these conditions, and due to the emerging demand by the interagency C-IED-related community of

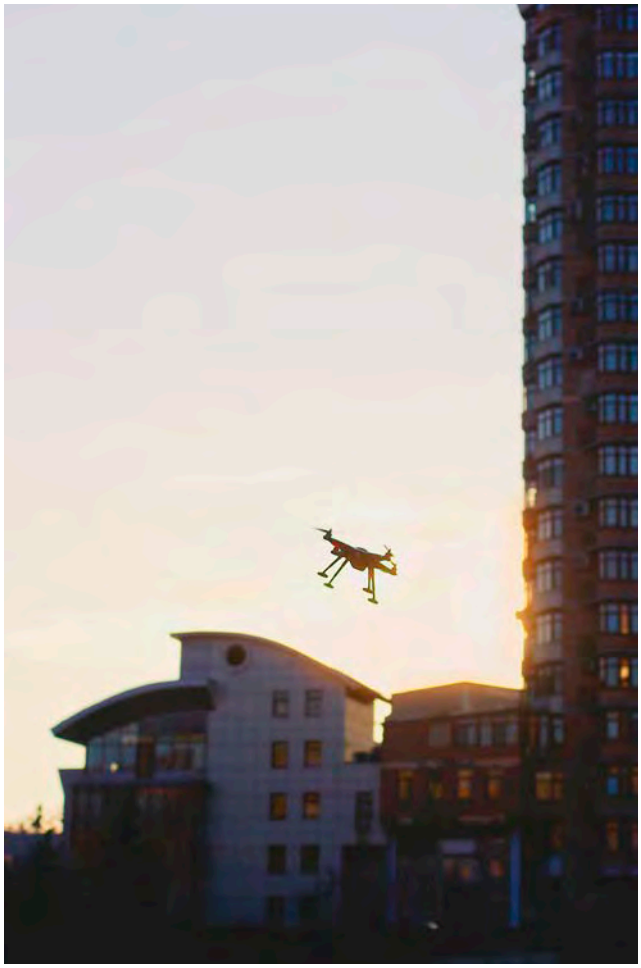
Figure 1 – Cover of several handbooks on drones published by INTERPOL (Source: INTERPOL)

interest, the C-IED Centre of Excellence is currently developing a combined project/experiment which embeds the identification of tools and procedures in support of the specific threat analysis, risk assessment and technical exploitation of explosive-laden drones, with an especial focus over NATO Class I UAS in general and small UAS (s-UAS) in particular.

The first portion of the project is merely an effort in the systematization of the experience of the C-IED COE subject matter experts (SMEs) in the analysis of threats from explosive-laden drones and its associated risk assessment, gained from 2014 on due to the continuous effort in identifying, studying, understanding and reporting the matter from Iraq, Syria and Ukraine areas of operations (e.g. the first C-IED COE reports on explosive-laden UAS were published in 2016).

But the most relevant initiative of the referred project consists of a deep study on the application of all the Technical Exploitation capabilities as defined in NATO doctrine (see AIntP-10{B} Allied Intelligence Publication "Technical Exploitation"), which is planned to finally conduct to a pilot course as its main output.

In fact, that training initiative is intended to provide the theoretical and practical framework for the students to understand how the application of Technical Exploitation could lead to the identification of trends, tactics, techniques and procedures in the adversary use of drones, as well as teaching how to recognize, categorize and evaluate essential design clues, electronics, components, configurations, programming and avionics along with the potential information with intelligence value which could be extracted from the overall application of TE capabilities (excluding MEDEX and CELLEX, which have their own training offered by NATO at the C-IED COE).



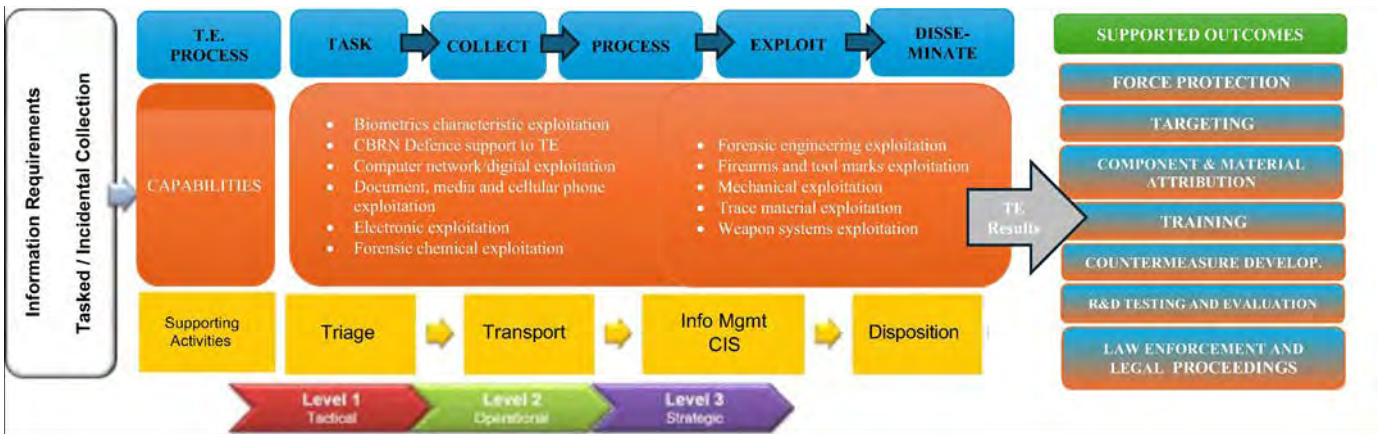


Figure 2 – NATO Technical Exploitation process (Source: https://doi.org/10.31374/sjms.333)

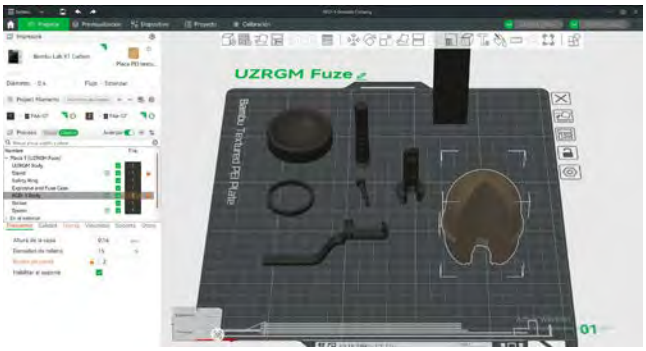
The C-IED COE 3D Repository: From Proof of Concept to Operational Capability

In 2023, the Counter-Improvised Explosive Device Centre of Excellence (C-IED COE) was selected to design, develop and launch a 3D database in support of NATO's Defence Against Terrorism initiatives. The aim of the project was to harness rapidly advancing 3D scanning and printing technologies to create accurate digital scans of devices and components in multiple formats, and to determine the most secure and efficient means of sharing them across the Alliance.

Over the course of two years, the Defeat the Device (DtD) Branch worked tirelessly to build the framework, implement comprehensive security measures, and populate the database with 3D models created both at the COE and in cooperation with NATO Partners. These efforts culminated in the official release of the C-IED COE 3D Repository on 1 October 2025, a milestone for the Centre and the wider C-IED community.

A New Era in Counter-IED Training and Collaboration

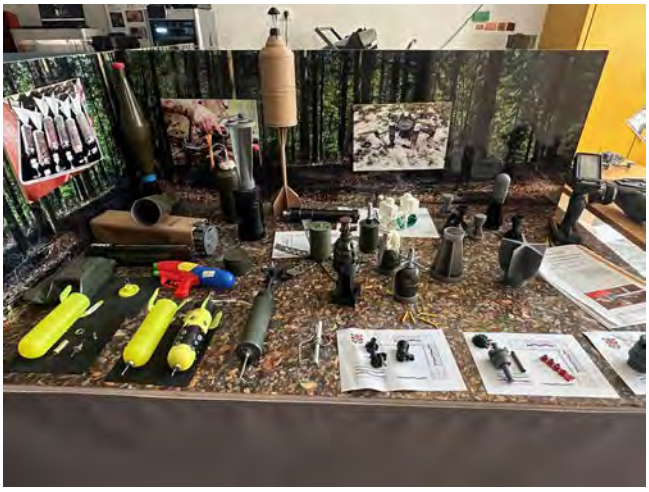
The C-IED COE 3D Repository represents a major step forward in how NATO and Partner Nations prepare for and respond to the evolving threat of improvised explosive devices (IEDs). This groundbreaking initiative



provides a cost-effective, scalable and responsive solution at the tactical level, enabling on-demand production of realistic training aids, replicas, and specialized components.

As modern warfare and technology continue to evolve, this dynamic capability ensures that training and operational readiness remain at the cutting edge. The initial proof of concept was to create a repository that offered a secure digital environment for sharing not only 3D-printable files but also essential supporting materials, such as technical documentation, event reports and best practices.

Through the development of the repository, the C-IED



COE aimed to strengthen the Alliance's ability to innovate, collaborate, and adapt to the changing threat landscape. Designed to be user-driven and mission-focused, the repository fosters collaboration through two-way file sharing, innovation and interoperability across the C-IED network.

Whether replicating an IED component for classroom instruction or producing mission-specific training aids in a deployed environment, the C-IED COE 3D Repository serves as a force multiplier enhancing readiness, adaptability and resilience throughout the Alliance.

Proof of Concept and Initial Response

The success of the proof of concept was evident upon its release. The response from NATO Allies and Partner Nations was immediate and enthusiastic, with a surge of requests for access and collaboration. Interest in the project extended far beyond military organizations.

National police forces, government agencies, academic institutions and industry partners have all expressed their desire to contribute expertise and resources to the repository. This broad engagement highlights the system's potential not only as an operational tool but also as a platform for cross-sector innovation and education in the field of C-IED technology.

Expanding Capabilities and Looking Ahead

While the program began with limited resources and required creative, adaptive solutions to progress, its trajectory continues upward. The C-IED COE is actively collaborating with a variety of NATO entities to expand and refine the repository, supported by a growing backlog of 3D files awaiting review and upload.

The Defeat the Device Branch is also developing an enhanced platform that will provide users with a more intuitive, efficient and secure experience. Concurrently, efforts are underway to expand access to additional Partners beyond NATO, further reinforcing the spirit of collaboration that underpins the initiative.
In addition, early-stage discussions are exploring training and education opportunities related to 3D printing, scanning and design. These could take the form of in-house courses or Mobile Training Team (MTT) offerings, with the aim of equipping personnel with practical skills to employ these technologies effectively within their respective organizations.

Conclusion

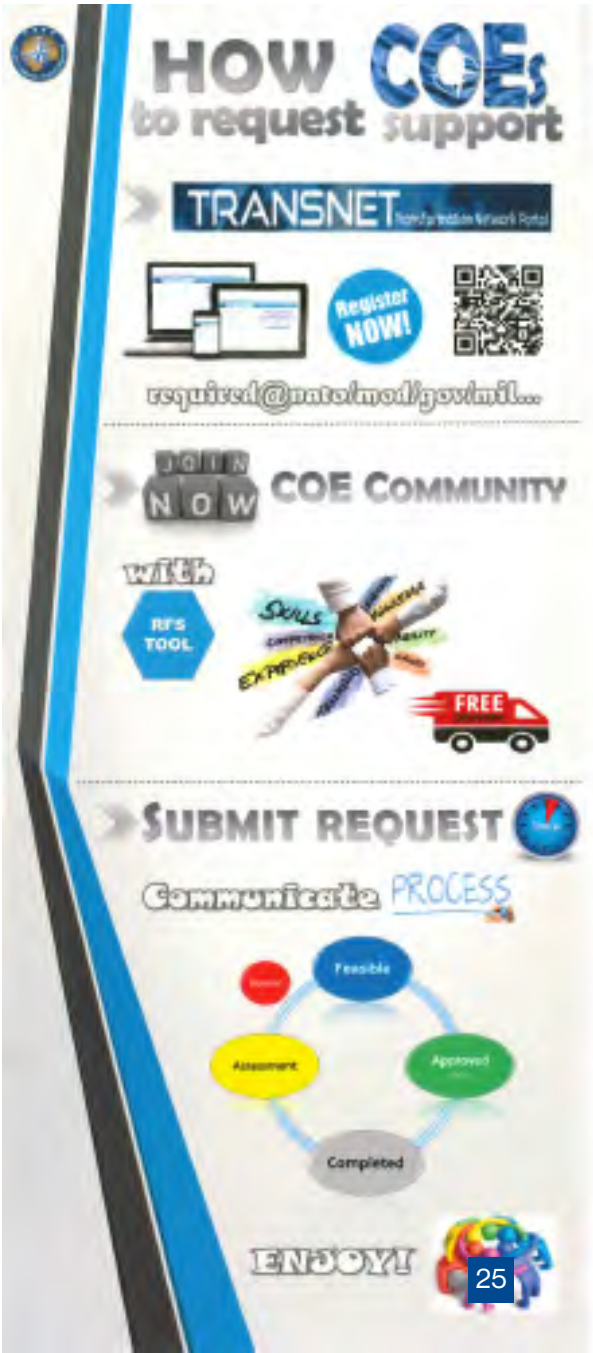
The creation of a secure platform for sharing educational materials, technical data, and training resources remains at the heart of the project. The 3D Repository empowers personnel across the C-IED community to continually advance their capabilities, adapt to emerging threats, and do so in a cost-effective, accessible and collaborative manner.

As global conflicts evolve, so must the ability to innovate and share knowledge. The C-IED COE remains steadfast in its commitment to providing the tools, expertise and education necessary to enhance the collective readiness and resilience of the NATO Alliance and its Partners.

By fostering collaboration and continuous innovation, the C-IED COE 3D Repository strengthens the Alliance, layer by layer, through shared knowledge, advanced technology and a unified approach to countering evolving threats.

Accredited 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

The challenge from Explosive-laden First-Person View (FPV) Drones

Since 2014, the explosive-laden drones based on modified commercial-off-the-shelf (COTS) models fitted with improvised munitions have progressively shown their potential capabilities in crisis areas, such as Iraq, Syria and Ukraine.

But it was during the Nagorno-Karabagh conflict in 2020 when the decisive role of the explosive-laden unmanned aircraft systems (UAS) in modern warfare was effectively evidenced. The combined use of aerial platforms with intelligence-surveillance-reconnaissance (ISR), weaponized drones with missiles and loitering munitions was able to "blind" the Armenian forces through the suppression of their air defenses and communications, letting the ground armament highly vulnerable.

In July 2023, a video from Ukrainian fighters showed the successful tactical use of a modified race first person view (FPV) explosive-laden drone against pro-Russian soldiers. This was possible taking advantage of the estimated protection of a building where the FPV explosive-laden drone was able to enter through the main door.

FPV drones are modular platforms made with commercial-off-the-shelf (COTS) or self-manufactured components, which makes them flexible and hard to track.

One of the main characteristics of any FPV small, unmanned aircraft system (s-UAS) is the high own-weight/payload ratio. For example, a 10-inch model can move an average payload of about 2.5 kilograms, while a 13-inch one can transport a 4.5-6 kilograms payload.

Such a high payload capability allows FPV s-UAS to use a large variety of explosive devices, with multiple effects, such as blasting, incendiary, 360° or directional fragmentation, thermobaric, anti-armor, obscurant... With a relatively short range for tactical purposes, their high speed and maneuverability are also valuable characteristics of FPV s-UAS.

Along with that, FPV s-UAS have an overall low (radar, thermal, sonic, visual...) signature which makes them

Figure 1 – Modified COTS UAS for dropping improvised munitions in Iraq (Source: @MitchUtterback)

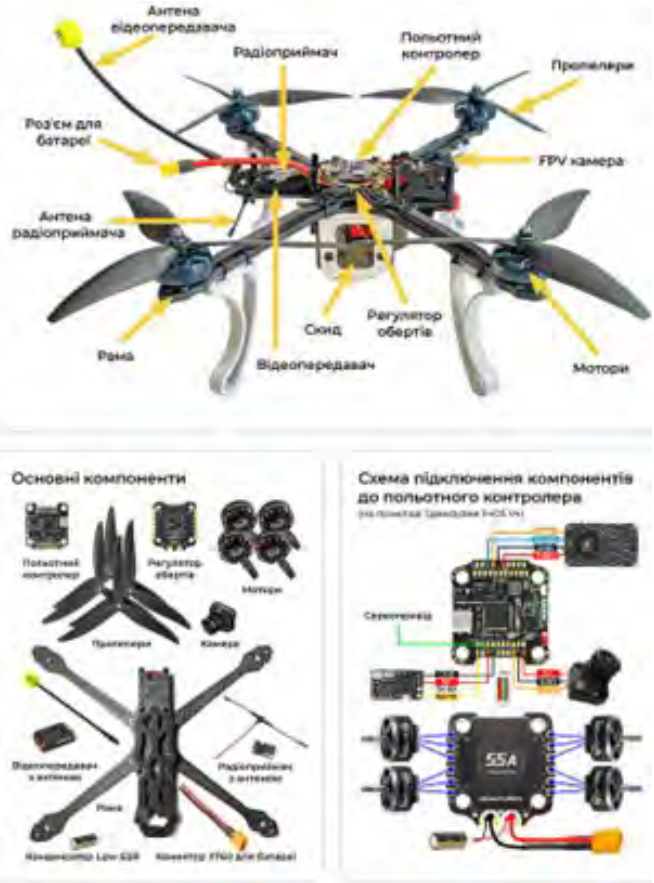


Figure 2 – FPV drone main components (Source : @VictoryDrones)

hard to detect with other means than merely their associated electromagnetic signature (e.g. used for control, communications, video).

However, current technologies are providing flexible and adaptive opportunities to FPV s-UAS regarding potential countermeasures against both detection and electromagnetic warfare: signal shielding, encryption/coding of signal, change of frequencies, autonomous navigation, alternation of different control systems, optic fiber guidance, filtering of jamming, radiometers, relay systems, use of mobile data networks, alternate waypoint systems and so on.

Additionally, the implementation of artificial intelligence through COTS microcomputers (e.g. RAPSBERRY PI, ARDUINO UNO, NVIDIA JETSON NANO) is allowing FPV s-UAS to reduce detection, identify electromagnetic patterns, optimize communications, improve autonomous guidance, process collected information, recognize/select targets, employ evasion techniques...

On the other hand, most of the ideas, technical information, components, manufacturing instructions and training tools for the tactical (or criminal) use of FPV s-UAS are publicly available through the Internet.

In fact, the wide and flexible use of explosive-laden FPV drones is effectively posing a game-changing challenge not only to modern warfare but also to homeland security.

Figure 3 – Russian FPV drones fitted with improvised munitions based on a modified TBG-7V thermobaric rocket warhead / cheap COTS microswitch used in the device (Source: @VictoryDrones & Aliexpress.com)

Figure 4 – Cover of manual on explosive-laden drone making shared by DAESH followers (Source: Matrix)

From Mines to Hybrid Threats: Lessons for Counter-IED and Force Preparation

The conflict in Ukraine highlights the rapid evolution of explosive threats and the logistic and doctrinal challenges they pose. Mines have shifted from conventional designs to advanced, tech-enabled systems integrated with unmanned platforms, blurring the line between industrial and improvised devices.

These changes demand adaptive strategies that combine technical solutions with operational foresight. This article explores the logistical impact of large-scale mine adaptation, key technological innovations, and reaffirms the relevance of Counter-IED (C-IED) principles for countering hybrid explosive systems in future operations.

Logistical Implications of improvised landmines in the Ukraine War

The war in Ukraine has triggered a profound transformation in the use and production of landmines, particularly from a logistical standpoint. As the conflict evolved and the stockpiles of Soviet-era mines—such as the TM-62—rapidly depleted, Ukraine was forced to adapt by developing a new generation of landmines. These include modernized versions like the TM-2025, innovative designs such as the Gingerbread, and locally produced copies of foreign models like the MON-50 or M18A1 directional fragmentation mines.

This shift created major logistical challenges. In 2022, supply chains were not prepared for large-scale combat or sustained munitions production. Necessity drove innovation: domestic manufacturing using technologies like 3D printing and frontline design improvements became vital.

Local production reduced reliance on foreign suppliers, shortened logistical chains, and improved flexibility, aligning with Jomini's principle of interior lines. Decentralized production enhanced efficiency and survivability by limiting vulnerabilities to unmanned aerial systems (UAS) attacks on supply routes. Overall, improvised mine development reflects wartime innovation driven by logistical needs, making domestic production a key defensive asset.

Wartime Engineering: How Technology is Redefining Conventional Mines as improvised ones

The static frontline spanning over a thousand kilometers has created unprecedented demand for landmines and explosive devices for unmanned systems. This reality has driven innovations to improve initiation systems, enable remote deployment via commercial platforms, and replicate designs for sustained availability: a pragmatic response to logistical constraints and the need for flexibility in modern warfare.

The introduction of advanced electronic initiation devices such as JONIK and VERBA in mid-2024 marked a significant turning point, the full implications of

which remain uncertain. These systems enable dual use, operating both with unmanned platforms and traditional IEDs. Their compact design, reliable performance, low power consumption, and integration of multiple inertial sensors (i.e. gyroscopes and accelerometers) or magnetometers, have driven widespread adoption by both sides in the conflict.

Continuous improvements based on operational lessons — exemplified by the incorporation of Doppler microwave motion detector fuzes, such as the Ukrainian DROP-2 model currently employed in modified OZM-72 antipersonnel landmines — have further enhanced their capabilities by enabling precise motion detection and reducing false activations.

Given the proliferation of variants and large-scale production, it is highly likely that, once the war concludes, these devices could appear in other conflicts or be exploited by Violent Extremist Organizations.

Modifications for deployment by UAS have introduced significant innovations in conventional mines design. Some of them have been adapted with tail assemblies to allow controlled descent from aircraft, improving accuracy and reliability, such as the well-known TM-62. In other cases, these tails have been added to ensure optimal functioning after impact, as seen with the previously mentioned OZM-72 or the refined POM-110 variant, designated K-2, developed by the 20th Brigade of Unmanned Systems.

Additional noteworthy innovations include the weight reduction of certain mines for use with commercial drones, such as box-type PMD models and, more recently, the integration of a 3D-printed wing into the improvised mine known as GINGERBREAD to enhance dispersion when UAS are employed for mining tasks. These adaptations not only increase the precision and flexibility of aerial delivery, but also pose significant tactical risks, as they enable rapid, remote emplacement of mines in contested areas, complicating detection and clearance operations.

Integrating C-IED Principles to Counter Next-Generation Explosive Systems

To conclude, Tactical and technological innovations, such as 3D printing, advanced electronic initiators, and integration with unmanned systems, have transformed improvised mines into complex, adaptive threats. While still inexpensive and asymmetric, they also present exploitable vulnerabilities through a robust C-IED approach.

C-IED's strength lies in integrating multiple enablers (intelligence, Explosive Ordnance Disposal, Electronic Warfare, cyber, logistics) into a coherent strategy that combines technical solutions with network disruption, supply chain interdiction, and layered protection.

This applies at both tactical and operational levels, ensuring immediate threat mitigation and long-term coordination. Ultimately, countering hybrid explosive systems requires technical adaptation, doctrinal innovation and multinational cooperation. Leveraging C-IED's integrative power across domains will be critical to building layered defenses against increasingly adaptive threats.

2025 Threat Dynamics by Human Networks

Although the huge reduction of hostilities between Israel and Palestinian militias has been evidenced in the last quarter of 2025, the potential global impact of the situation in Gaza Strip and the West Bank continues being relevant regarding the extremist violence.

Nonetheless, the convergence of the conflict in Gaza with other geopolitical matters has been reflected in the 2025 metrics on detentions, attacks and dismantled plots related to religiously motivated extremist violence in European and Northern American territories, which are currently showing a huge increase compared with previous years.

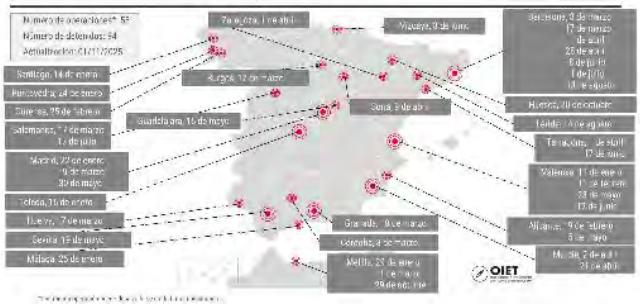


Figure 1 – Operations/detainees for religiously motivated extremist violence in Spain in 2025 (Source: OIET)

Without any doubt, the African continent has taken the worst part of the threat evolutions during 2025. Nigeria has the annual world record concerning attacks, while the Sahel has been the area where non-state actors have been gaining more terrain control, relevance and opportunities for alternative governance.

Regarding Mali, Jamāʿat nuʿrat al-islām wal-muslimīn (JNIM) has carried out a smart strategy, blocking the main supply routes to the capital and other relevant urban centres, strangling the internationally isolated ruling military junta, as it has restricted dramatically the access to fuel. JNIM is also threatening the capital city in Burkina-Faso, while Niger is not able to effectively fight the terrorist threat.

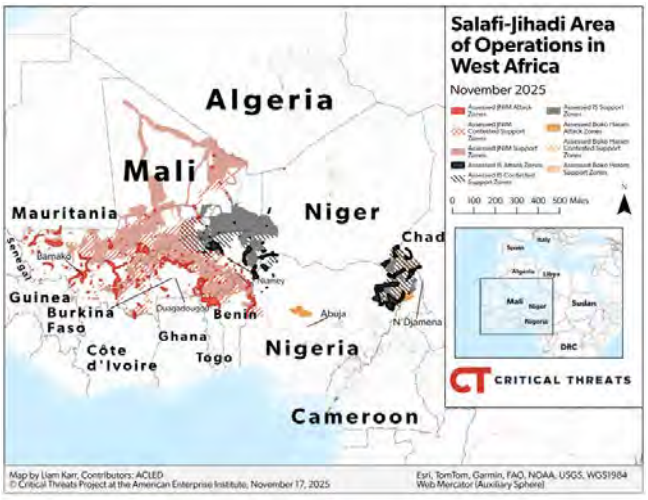


Figure 2 – Areas of operations of adversary human networks in Sahel & West Africa (Source: CT)

On the other hand, the Tuareg Front for the Liberation of Azawad (FLA) is pressing the Malian government from the East through a very effective use of new tactics, techniques and procedures, such as the use of explosive-laden first-person view (FPV) drones, both in ambushes and surgical attacks.

Due to the return to hostilities between DAESH in West Africa Wilayat (ISWAP) and the two main remaining factions from former Boko Haram (JAS) group in Lake Chad Basin, the security situation in Nigeria, Cameroon and Chad has not improved.

The conflicts in Sudan and the Democratic Republic of Congo are still alive, while the threat by DAESH Mozambique has been growing during 2025. Al Shabaab in Somalia (which is apparently in contact with Ansar Allah in Yemen) is gaining relevance, although the weakened DAESH Somalia has been suffering from the pressure of the Somalian forces, which is supported by the United States.

The rest of African regions affected by irregular threats have not significatively improved their respective situations.

With regards to Central Asia, last reports indicate a potential support to Al Qaeda and other terrorist groups by the Islamic Republic of Afghanistan, along

with a prudent posture from DAESH in Khurasan and disputes with Pakistan.

Figure 3 – Map of "The Great Afghanistan" published by the Afghan government (Source: CT)

Pakistan is subject to the threat posed by several groups, being Tehreek i Taliban Pakistan (TTP) the predominant one, although it also acts inside Afghanistan.

Meanwhile, the use of improvised explosive devices (IEDs) is still notable in Myanmar, where the insurgency is challenging the governance of the military junta. In fact, it currently ranks third worldwide (after Russia and Ukraine) in reported explosive-laden drone attacks.

Figure 4 – Myanmar fighters with an explosive-laden drone (Source: X)

On the other side of the world, the use of IEDs from unmanned aircraft systems (UASs) is dramatically growing in the hands of drug cartels, both against their opponent cartels and the governments of Mexico and Colombia.

And finally, we should accept that the use of IEDs in Ukraine and Russia has been growing from 2014 on, contrary to the assessment of many military sources.

Nowadays, it looks like the C-IED approach is not only still valid, but also essential to anticipate threats, as well as to assess how to reduce, reject or impede the capabilities of adversary human networks.

Online capabilities in support of additive manufacturing of IEDs

It is well known that the Internet is full of designs, practical instructions and files for the manufacture of improvised weapons using 3D printing technologies and means: impact weapons (as kubotans, knuckledusters, maces, sticks...), stabbing/cutting tools (knives, punches, icepicks...), stocks, handles, loaders, rails, mounts, magazines, select-fire switch sears, gun frames, cartridge cases, suppressors, and even complete firearms for small calibers.

Figure 1 – Different types of seized 3D-printed weapons or their parts (Source: British Columbia CFSE Unit)

Those referred techniques used to print pieces of artwork with ornamental or practical aims utilizing different specific printers and materials are not only useful for industrial, didactical or entertainment purposes, but also able to provide criminals, fighters and terrorists with uncontrolled and easy-to-produce components for manufacturing weapons.

A fact that is less publicly known is that open sources are also allowing access to blueprints and technical instructions for components of improvised explosive devices and/or modified munitions.

In principle, and almost without any potential alert or tracking by investigators, anyone with a computer could acquire a 3D-printer, find a free (or paid) design of choice in the internet, buy the respective filaments (with different percentages of plastics, resins, metals, composites, wood, ceramic...), follow the assessment by other users through the web and, after several tests, finally manufacture a hazardous device able to shot or detonate with the addition of commercial (also improvised) munition or any sort of incendiary and even explosive mixture.

Currently, you do not need to seek the Darknet to find both blueprints and instructions to have access to your own 3D-printed weapons. There are not only specifically dedicated websites for 3D-printed firearms and their parts (e.g. DEFCAD, 3Dgunbuilder, ctrlpew, printyour2a, 3dprintedgungear, topboyghostguns, hammy3dprints...), but also multiple sites that contain 3D-printing designs, including components for firearms or sometimes almost complete weapons, disguised between legal 3D replicas (e.g. cults3d, printables, stlfinder, yeggi, free3d, thinginverse...).

Along with that and, under confusing labels, such as FOSSCAD (Free Open-Source Software & Computer Aided Design), some online communities are sharing designs for 3D-printed guns or even selling 3D-printed weapons or their parts almost without any banning (e.g. reddit, telegram, facebook...).

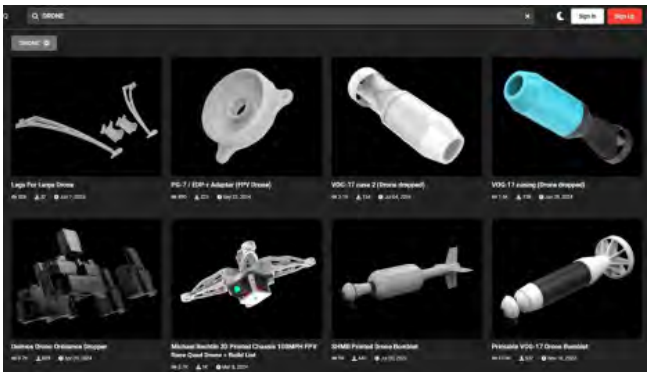


Figure 2 – Instructions & files on 3D-printed improvised munitions for drones (Source – DEFCAD)

A quick search inside websites, such as DEFCAD, could guide to additive manufacturing of several IED-related components as improvised munitions for drones, hand grenades, landmines, rockets, switches, homemade fuze systems, adaptors and even mortars.

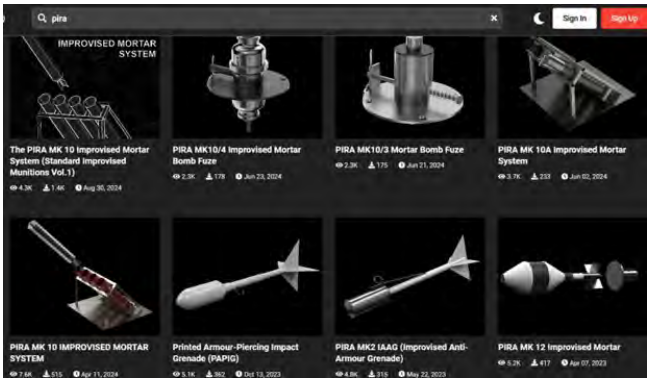


Figure 3 – Instructions & files on 3D-printed improvised mortars formerly used by terrorist groups (Source – DEFCAD)

Additionally, the public availability of different types of filaments with metal content (e.g. copper, aluminum...) could support not only the production of metallic parts for weapons, but also the homemade production of metal liners for improvised explosive devices.

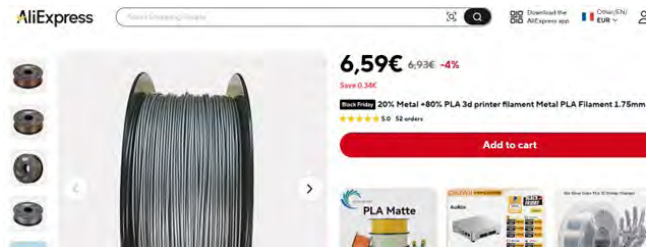


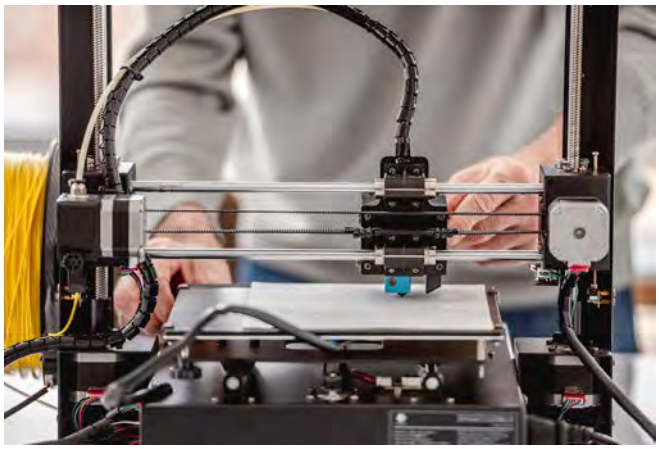
Figure 4 – 20% metal 3D-printer filament (Source – AliExpress)

On the other hand, both sides of the Ukrainian conflict are widely and openly sharing terabytes of data regarding the battle-proven employment of additive manufacturing in direct support of the fabrication and use of improvised explosive devices.

In Myanmar, several militias fighting against the governing Military Junta are extensively using not only 3D-printed improvised munitions for unmanned aircraft systems (UAS), but also fully equipping units with the FGC-9 3D-printed 9mm Parabellum firearm.

In parallel, religiously motivated violent extremist organizations (e.g. DAESH) are already sharing files and instructions about this topic, and they are showing a growing interest in manufacturing 3D-printed weapons and devices.

With the strong impulse given by the Ukrainian conflict, and the difficulty of tracking information and components, the easy public access to 3D-printing capabilities for both firearms and improvised explosive devices is not announcing a quiet close future to counter terrorist and criminal activities.



Use of Artificial Intelligence (AI) in support to IED Systems' Capabilities

2. NATO's 2021 AI Strategy set out a Strategic Vision, with four Aims and six Outcomes. Within the AI Strategy, Allies endorsed six Principles of Responsible Use (PRUs) for AI in Defence, i.e. Lawfulness, Responsibility and Accountability, Explainability and Traceability, Reliability, Governability and Bias Mitigation.

In this article, in order to avoid self-imposing intellectual limitations by constraining ourselves to Improvised Explosive Devices (IEDs) systems, we will deal with the use of AI on the battlefield of a 5th generation warfare (according to Daniel Abbott's definition) or in the gray zone. We will focus on human networks, as Attack the Networks (AtN) is the main pillar to consider if we want to anticipate the threat posed by the IED systems.

Among the priorities in NATO regarding the nine Emerging Disruptive Technologies (EDT), AI is currently perceived as the main one, but on the one hand, it is still subject to the ups and downs of the industry and, on the other hand, it should be subject to Law (both International and National) and Ethics. In fact, the inclusion of AI in Article 36 "New Weapons" of Protocol I to the Geneva Convention should be considered.

An important issue to have in mind is that the available commercial AI is not valid to use on the battlefield, precisely because we need to avoid these ups and downs and because the AI must be trained effectively, efficiently and focused on AtN.

During 2025, the response rate "with content" of the different commercial AIs has been raised to 100%, which means that they will always respond, even if this implies a higher rate of hallucinations. This cannot be allowed on the battlefield, where a mistake is ammunition for the opponent's Strategic communication (STRATCOM) and can cost valuable human lives of our own.

To this, we must add that AI must be nourished by public data, but also by either classified data or classified information and of course, it must not have an exposure surface to the internet for cybersecurity reasons.

The Israeli Defense Forces have probably been the most proactive actors in the extensive use of AI on the battlefield. Several social media outlets, citing Israeli and Palestinian sources, have reported on a linguistic recognition AI trained not only in formal Arabic, but also in local dialects, which allows a holistic study of internet posts, text messages and other information niches to establish the mood and foreseeable reactions of the civilian population to actions of war.

This is an application that is operational and a priori, respectful of the Law and a clear example of actions in the cognitive environment.

We can see another example in Ukraine, where facial recognition was used for the first time in conflict zones to establish a Positive Identification of Russian soldiers, even with their faces partially covered or with facial wounds.

It would be interesting to use the results of this type of reconnaissance as Battlefield Evidence, which would make it possible to bring war criminals to justice. Another interesting application would help in the field of Cultural Protection of national heritage, which is an issue that currently concerns many countries.

Moving away from existing conflicts and entering the theoretical world, the use of AI is a magnificent tool that, based on sociological, ethnological, environmental studies and all those disciplines that can provide data or information, elaborates patterns of life and even define exact geographical locations.

This information is essential for the advanced development of a target when the entity is human. This is perhaps the most controversial aspect of the use of AI, even if it does not execute a lethal kinetic attack.

But it is possible to go deeper into the fight against Human Networks. Even though it is almost a utopia, there is a possibility to train an AI to elaborate hypothetical scenarios on how a human network would evolve if one or more of its elements were removed from the operating environment and even, on how it would affect not only the network, but also the cognitive environment if this withdrawal occurred in a certain sequential order of actions.

In the same way, changes in Tactics, Techniques and Procedures (TTP) could be predicted through the information obtained from the available resources, either locally or through the smuggling of goods, the dissemination of knowledge, or any other circumstance that may affect the actors thus modifying the operational environment.

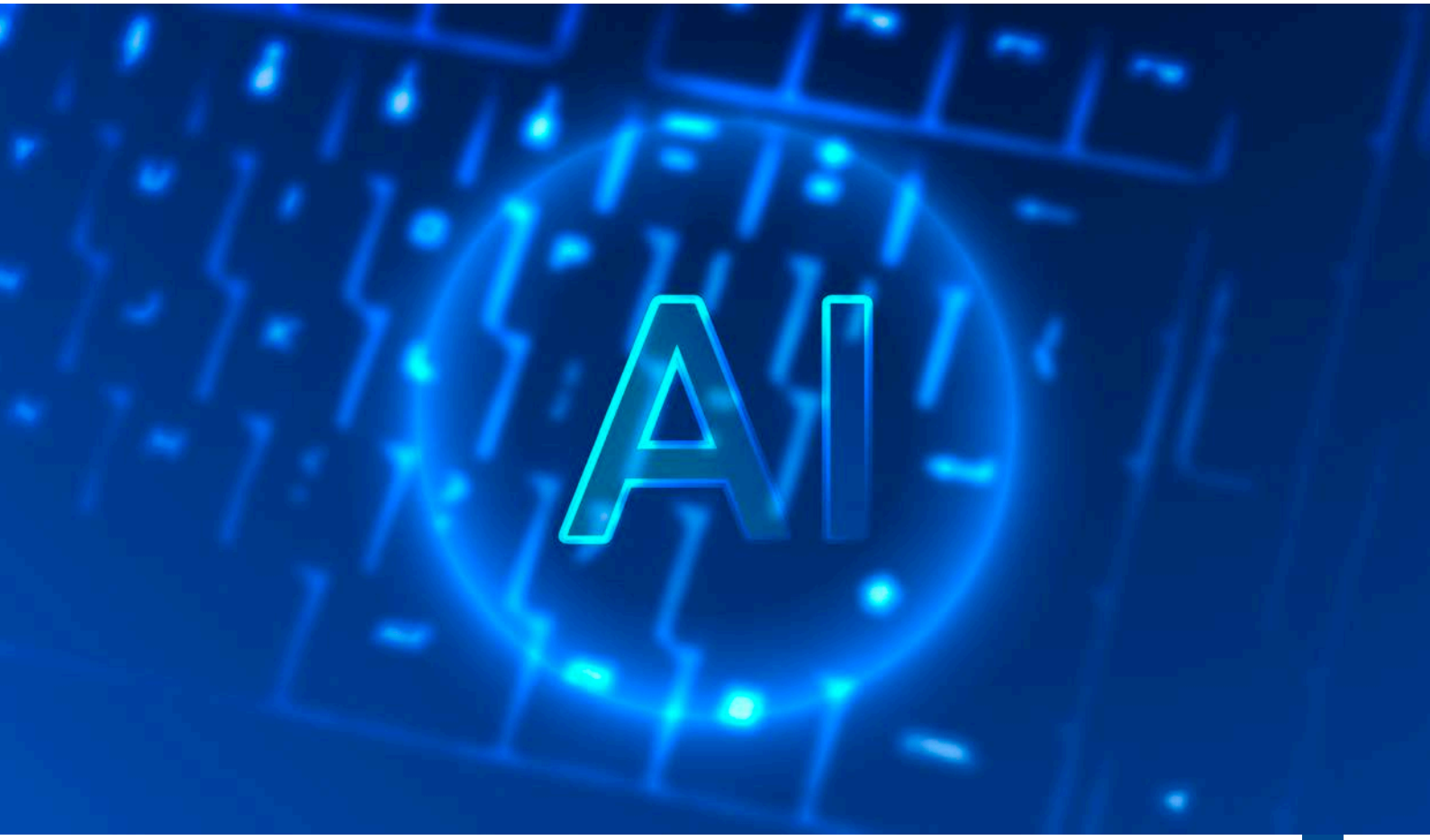
In the scenarios described above, the risks to be assumed would be, on the one hand, the kind of knowledge provided to the AI and, on the other hand, the need to make sure there is a total absence of bias.

In short, the desired second and third order effects could be obtained by minimizing one's own casualties and collateral damage, always using the minimum amount of armed intervention, which would benefit the cognitive environment and allow a secure and safe environment in the Area of Operations by performing a "Battle Damage Assessment" procedure without even launching a single operation.

All of this must be subject to the supervision of human analysts (from intelligence or operations branches) trained in AI, and then go through the validation of the operation's commander, in order to avoid hallucinations or contamination due to disinformation.

But there are limits. Under no circumstances in the current state of the art, should automation with AI be incorporated to autonomous weapons, according to the recommendations of the United Nations General Assembly in its report "Lethal autonomus weapon systems", since most of the work to be done in this field is related to the legal and ethical aspects. In fact, this report includes the use of "Responsible Artificial Intelligence in the Military Domain Process".

In conclusion, when we talk about Human Threat Networks, AI, in support of IED Systems' Capabilities or in support of AtN, is a new tool whose limits are only Imagination, Ethics and Law.



C-IED/AtN Integration Experiment

One of the main potential mistakes that the C-IED Community of Interest has been traditionally subject to (and probably the worst message that can be sent) is to consider tactical Explosive Ordnance Disposal (EOD) or Military Engineering (MILENG) exercises as "C-IED exercises".

In fact, EOD and MILENG are essential enablers to C-IED at the Tactical level when conducting operations, but C-IED is essentially conducted at the Operational level, and C-IED (as defined by NATO) consists of more activities and processes than those merely (and reactively) applied "at the left of the boom".

Tactical exercises, such as "Bison Counter" series (an EOD/MILENG based exercise promoted by the European Defense Agency (EDA)), "Northern Challenge" series (a NATO EOD exercise), "Ravens Challenge" series (United States of America EOD interagency exercise) or "Ardent Defender" series (a Canadian EOD-centric exercise) are for sure not the adequate frame to apply the whole C-IED cycle of processes.

Nonetheless, it is relevant to highlight that the C-IED COE made a huge (and unprecedented) effort to implement the C-IED processes at operational level with some sort of manned Joint Task Force Headquarters (JTFHQ) as secondary training audience inside the exercise "Bison Counter 2023" held in Zaragoza, Spain.

Although that initial test was merely a humble first step, it provided relevant outputs, such as a Standard Operating Procedures (SOP) for technical exploitation management, along with an additional SOP for C-IED processes at Joint Task Force level.

Figure 1 – "Bison Counter 2023" exercise's badge (Source: www.defence-industry.eu)

On the other hand, our Canadian colleagues are carrying out an outstanding activity trying to improve the application (and experimentation) of the Allied Technical Exploitation framework inside "Ardent Defender" exercises in all its editions.

It is worth mentioning their valuable test of a sort of Analysis Cell progressively trying to connect the EOD-centric TE outputs with an initial Intelligence analysis.

When developing "C-IED exercises", if we keep on focusing the conversation on the past experiences in Afghanistan and Iraq, we promote this wrong and obsolete approach to C-IED: it is not an end by itself, but just an approach, a mindset or a way of working which could effectively support (and improve) multinational and national operations where the threat derived from non-state actors (or those state-promoted) could have a significant role.

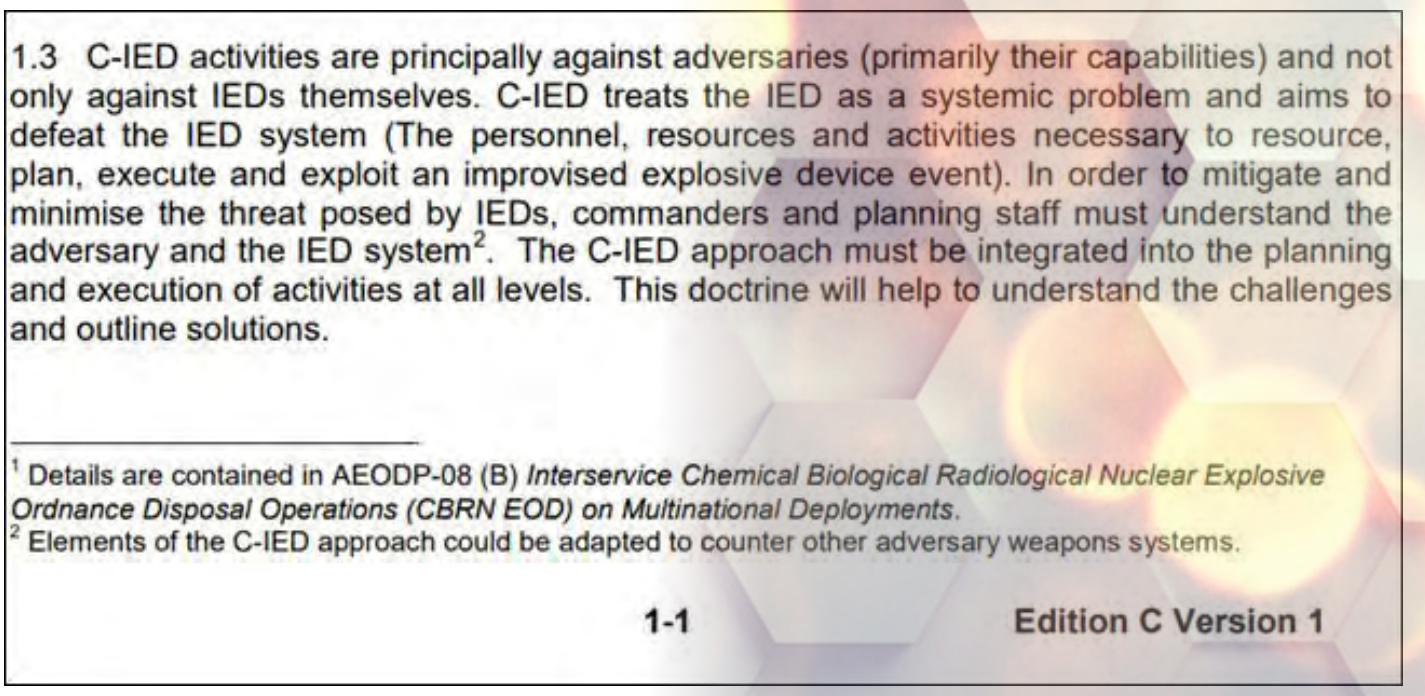
Yes, we are talking about "actors" and not about "IED incidents", as C-IED directly fights against the "IED systems" and therefore, against "those human networks behind the potential or effective use of IED".

It is absolutely viable to implement C-IED processes in an exercise without any sort of IED incident, but when the activities by adversary human networks could mean the achievement of capabilities to employ IEDs in a future, that is called C-IED "Attack the Networks", that is, a series of proactive and anticipatory activities trying to avoid the potential IED threat that pose a crude reality inside the area of operations.

The first trials to achieve this goals (e.g. "Northern Solution 2024") did not reach the level of expectation set by the Centre. As a higher level of Technical Exploitation management is desired during exercises connected to EOD collective training, the C-IED COE is currently trying to design and implement the C-IED approach and associated processes into Allied exercises at operational level under the denomination "C-IED/AtN Integration Experiment"

The planned output of the referred experiment would be a test-bed command post exercise (CPX) in which all the C-IED processes integrating Intelligence with Operations and Plans will be implemented, conducted and evaluated.

The expected primary training audience will be based on those essential to C-IED elements of a Joint Task Force Headquarters (Operational level) with the relevant elements of the Strategic level (e.g. SHAPE) and those at Upper Tactical level (e.g. Component Commands or Regional Commands Headquarters) as secondary training audience. We will see!



1.3 C-IED activities are principally against adversaries (primarily their capabilities) and not only against IEDs themselves. C-IED treats the IED as a systemic problem and aims to defeat the IED system (The personnel, resources and activities necessary to resource, plan, execute and exploit an improvised explosive device event). In order to mitigate and minimise the threat posed by IEDs, commanders and planning staff must understand the adversary and the IED system[2]. The C-IED approach must be integrated into the planning and execution of activities at all levels. This doctrine will help to understand the challenges and outline solutions.

[1] Details are contained in AEODP-08 (B) *Interservice Chemical Biological Radiological Nuclear Explosive Ordnance Disposal Operations (CBRN EOD) on Multinational Deployments*.
[2] Elements of the C-IED approach could be adapted to counter other adversary weapons systems.

1-1 Edition C Version 1

Figure 2 – Capture from NATO C-IED doctrine talking about the C-IED scope (Source: AJP-3.15(C))

Online propaganda dynamics by Violent Extremist Organizations 2025

After the dramatic increase of online propaganda (e.g. videos, digital magazines, posters, traditional religious songs...) calling for attacks over Western countries, democracies, other ideologies, Israel, and/or pro-American regimes from religiously motivated extremist violent groups during 2024 and early 2025, last months have witnessed a relative decrease in the publication and distribution of propaganda through the Internet.

Nonetheless, the threat is still alive, although less "propelled" by violent messaging. In fact, the amount of information related to improvised explosive devices manufacture and use has been growing during 2025, and the number of detentions and dismantled plots in Europe, connected with that religiously motivated extremist violence, has also been higher than it was during 2024.

Figure 1 – Call for attacks by Al Saqri Foundation for Military Sciences (Source: Matrix, April 2025)

One of the most relevant changes compared with previous years has been the huge decrease in the production of propaganda in English by DAESH in Khurasan Wilayat (IS-KP) through their media office Al-Azaim Foundation. For instance, the last published edition (46th) of "Voice of Khurasan" digital magazine was launched in June 2025, most probably due to the detention of a Canadian national behind a multinational cell of Al-Azaim. This has not prevented though that the Asian regional office is still producing the Urdu version of the referred magazine.

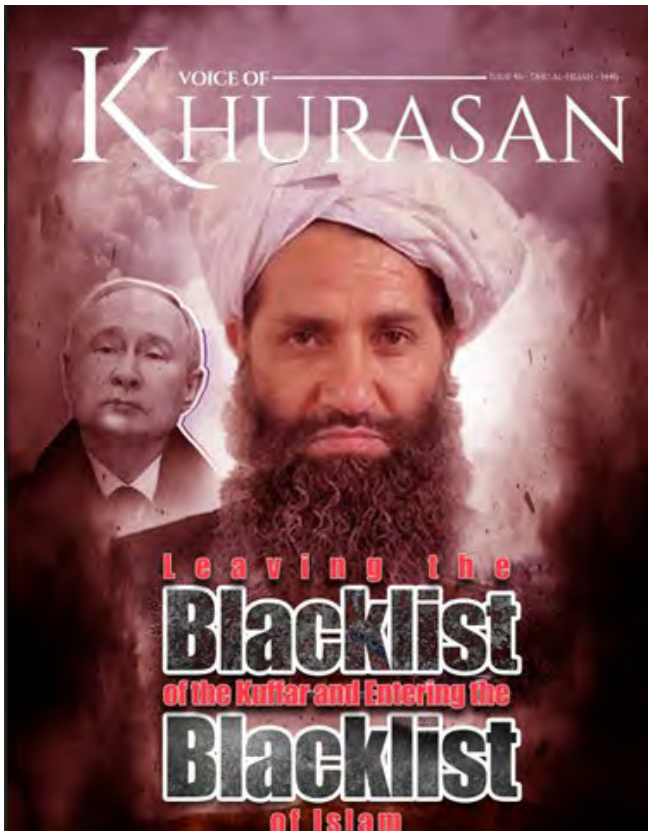


Figure 2 – Cover of 46th issue of the digital magazine "Voice of Khurasan" (Source: X, June 2025)

Meanwhile, the weekly news publication of the DAESH newsletter "An Naba" has been consistently maintained every Thursday during 2025, in the aim of presenting a more graphic than written source of information regarding the operations conducted by DAESH all around the world.

As the African continent is the area where attacks and territory control by DAESH is currently more patent, there has been an increase in the calling for support and "holy" migration (hijrah) to the Sahel area.

Figure 3 – Metrics on DAESH operations during first half of 2025 by Amaq Agency (Source: X, July 2025)

With regards to Al Qaeda, the activity has been more dynamic than it was during 2024: new digital magazines were launched (e.g. "HIJRA" by Al-Ghazi Foundation for Media Productions) and even three editions (9th, 10th & 11th ones) of the "INSPIRE GUIDES" by Al Malahem were published.

Figure 4 – Covers of "HIJRA" & "INSPIRE GUIDE 11" (Source: RocketChat, September-November 2025)

Meanwhile, and although allocated inside the overall AQ "enterprise", Jamāʿat nuʿrat al-islām wal-muslimīn (JNIM) has stablished its own influence campaign on other associated media offices under the leadership of Az Zallaqa

Figure 5 – Metrics on JNIM operations 22SEP-23OCT2025 by Az Zallaqa (Source: Chirpwire, October 2025)

In the specific case of Tehrik-e-Taliban Pakistan (TTP), they are still active in the production of posters, videos and digital magazines, as well as in the conduction of a relevant number of attacks in Pakistan and neighbor countries.

Figure 6 – Metrics on TTP operations during 1st half of 2025 (Source: www.newsvibesofindia.com, July 2025)

As a summary, the influence operations by religiously motivated violent organizations seem to be relatively decreasing at the end of 2025, but the currently evidenced propaganda calling for lethal actions and the online resources offered to carry out attacks on the Alliance assets are posing a relevant threat.


حملے 1377
رواں سال (2025ء) ماہ جنوری تا جون (شش ماہی) جمادی الثانی – محرم الحرام) میں تحریک طالبان پاکستان کی کارروائیوں کی تفصیلی رپورٹ
دشمن کا جانی نقصان
1940
832 ہلاکتیں
1108 زخمی
گرفتاریاں 57
نوعیت عملیات
اسٹنگ/ٹیر حملے 532
کورپلہ حملے 436
گھات حملے 113
دوہری حملے 74
گرنیڈ/بم دھماکے 34
تصادمی حملے 82
ٹارگٹڈ حملے 47
میزائل حملے 17
استشہادی حملے 02
نقصان اٹھانے والے ادارے
فوج/ایس ایس جی 932
ایف سی 517
پولیس/سی ٹی ڈی 450
خفیہ/امن کمیٹی 41
دشمن سے حاصل شدہ سامان
مختلف ہتھیار 74
میگزینز 20
گاڑیاں 38
موٹر سائیکل 36
ڈرونز 03
وائرلیس سیٹ 03
راکٹ لانچر 03
تھرمل/نائٹ وژن دوربین 02
موبائل فونز 02
بیگ/ایل ایم جی 02
مارٹر 01
ہزاروں گولیاں اور دیگر عسکری ساز و سامان
تخریب
اسلحہ ڈپو 01
ٹینک 03
وائرلیس سسٹمز 03
انٹرنیٹ/وائی فائی سسٹم 07
موٹر سائیکلیں 05
ڈش انٹینا سسٹم 08
بکتر بند گاڑیاں 07
ڈرون کیمرے 26
فوجی تعمیرات 22
سولر سسٹم 41
فوجی گاڑیاں 125
سی سی ٹی وی کیمرے 246
صفحہ - 1
تحریک طالبان پاکستان

ondata INTERNATIONAL | red seguridad

7th EDITION

NEW EDITION

2026 ONDATA CONGRESS & EXPO

DIGITAL FORENSICS & CYBERINTELLIGENCE

Digital Forensics & Cyberintelligence

The annual event for professionals, researchers and intelligence analysts from public organizations, law enforcement agencies, and major companies that rely on cyber intelligence, cybersecurity, and computer forensics solutions.

- Trends, technologies, and case studies.
- Digital investigation, OSINT, AI, and analytics. Legal interception and criminal investigation.
- Cybersecurity, threat detection, and mitigation.
- Dark web investigation and blockchain transactions analysis.

FEBRUARY 18 - MADRID

www.ondata.es/congreso

Online resources in support to IED-related plots 2024-2025

The current year has evidenced a trend in the increase of IED-related information published and disseminated online, compared to the figures identified in 2024.

Such information was not only related to religiously motivated extremist violence but also to current conflicts, accelerationism, anarchism and organized crime, among others.

Compared with the evolution from 2023 to 2024, last 12 months have evidenced a relative decrease in the activity developed by religiously motivated extremist violence forums and social media, while the dissemination of IED-related information has increased.

From Al Qaeda perspective, the online dissemination of manuals has not been quite relevant, but from DAESH side, the intensity in this area has been maintained: several published digital manuals (at least three of them) were even specifically including instructions for the manufacture of explosive-laden unmanned aircraft systems (UASs).

Figure 1 – Cover of manual by Al Saqri Foundation for Military Sciences (Source: Matrix, December 2024)

The most active DAESH-related publishers of online information regarding the manufacture of improvised explosive devices and/or homemade explosives were based on RocketChat and Matrix social media (e.g. Lamanho group, Al Saqri Foundation for Military Sciences office, "The Cook" user...).

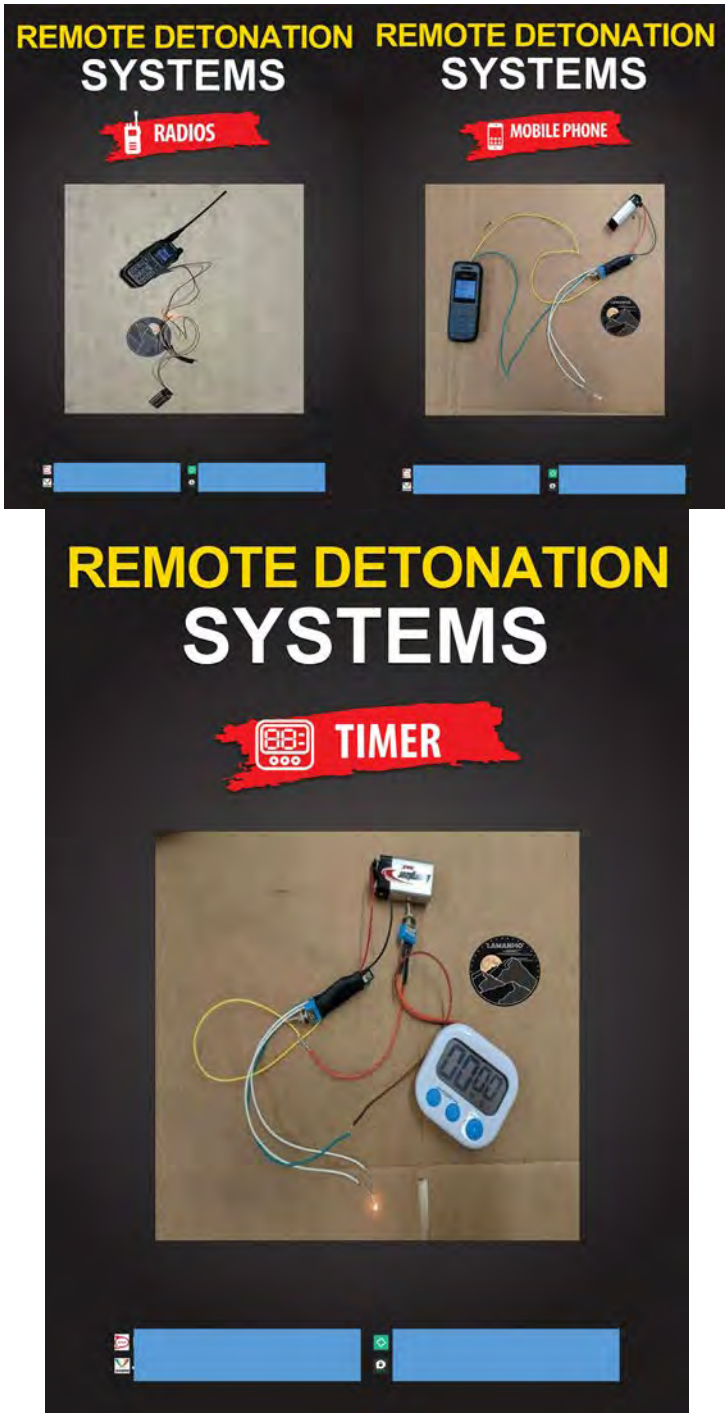


Figure 2 – Covers of manuals published by LAMANHO (Source: RocketChat, September-November 2025)

On the other hand, anarchist sources have been publishing and redistributing digital material for homemade explosive manufacture and simple devices.

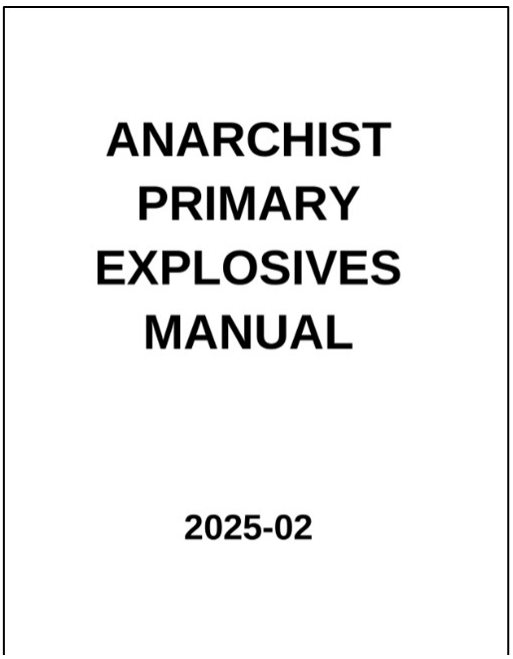


Figure 3 – Cover of an anarchist manual on homemade explosives (Source: Neversleep, February 2025)

But the most prolific 2025 online source for instructions, tutorial videos, manuals and ideas regarding improvised explosive devices has been provided by the supporters of both sides in the Ukraine-Russia conflict.

Coming from different approaches, we could find critical pieces of information regarding the use of IED: from the manipulation of military fuzes to the production of homemade incendiary mixtures; from the 3D-printing of improvised munitions to the use of vehicle borne IED; from homemade explosives to the use of mobile data networks for activating an IED; from technical instructions for victim-operated switches to the reconfiguration of a small explosive-laden unmanned aircraft system (UAS) to make it less vulnerable to electromagnetic warfare.

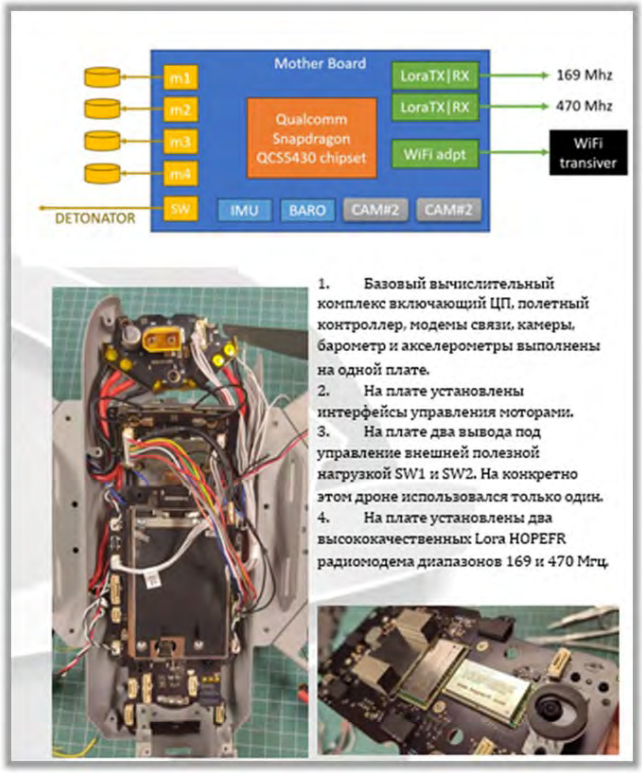


Figure 4 – Page of a manual for explosive-laden drone manufacture (Source: Telegram, August 2025)

In 2026, we will have to see how active violent extremist organizations will be regarding the publishing and diffusion of technical material for IED/HME manufacture.

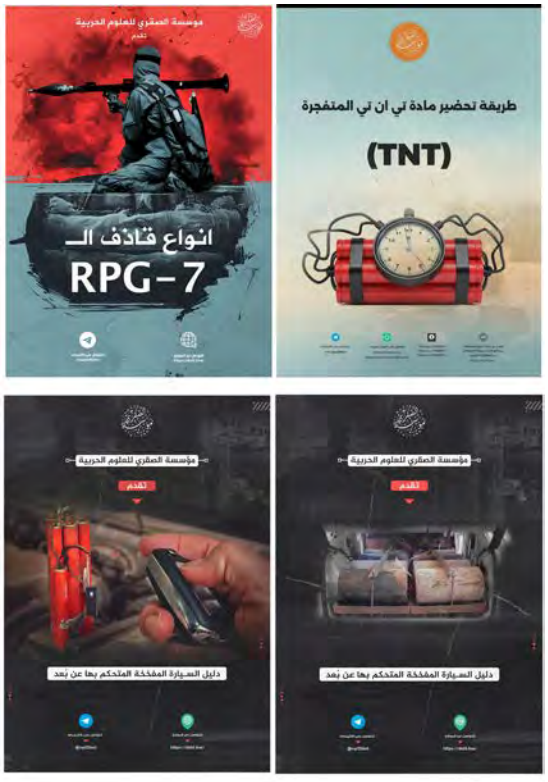


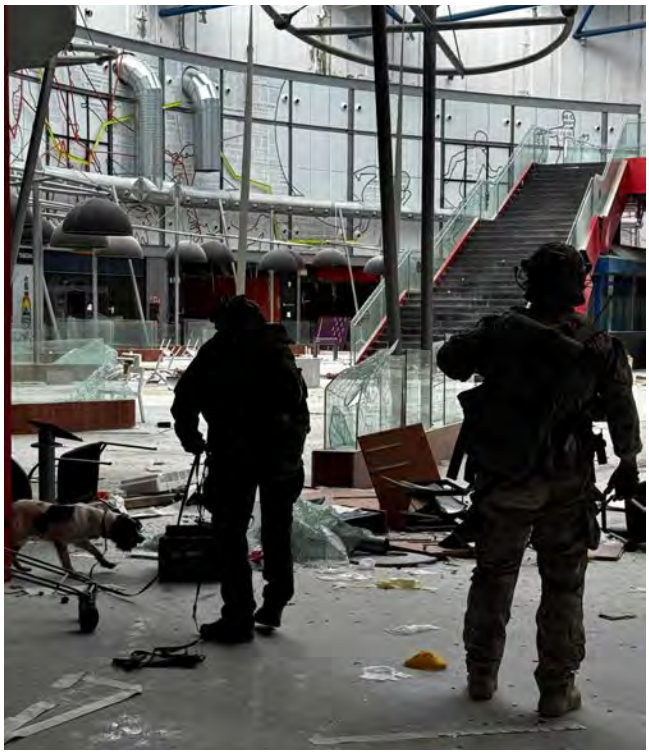
Figure 5 – Additional manuals by Al Saqri Foundation for Military Sciences (Source: RocketChat, 2025)

The potential role of C-IED in support of Article 5 Operations

Introduction

On 4 April 1949, the 12 original NATO members signed the North Atlantic Treaty. The core of this Treaty is its fifth article, which establishes the basis for collective defense in the event of an armed attack against one of the Allied nations. The Treaty also imposes geographical limitations on the area in which such an attack would be considered to trigger Article 5. It is limited to the European and North American territories of the Allied nations, with certain exceptions for some territories located outside Europe and North America.

The most recent NATO Strategic Concept, approved during the 2022 NATO Summit in Madrid, describes the Russian Federation as the most significant and direct threat to the Allies. It explicitly addresses the possibility of a Russian attack against Allied sovereignty and territorial integrity. Notably, it highlights how the Russian Federation seeks to establish spheres of influence and direct control through coercion, subversion, aggression and annexation, employing a combination of conventional, cyber and hybrid means against Allies and Partners.



These documents, together with lessons observed from the Russian invasion of Ukraine, help outline the scenario of a potential Article 5 operation: a Russian attack on Allied European soil using conventional and non-conventional means across all domains, affecting the entire European territory. This scenario also provides a starting point to discuss the potential role of C-IED in support of Article 5 operations.

The Evolution of the IED Threat

In the above-mentioned scenario, the IED threat could materialize in two distinct areas: the front lines, where conventional forces confront each other; and the rear areas and European depth, where non-conventional, cyber and hybrid means may be employed.

The IED threat is evolving from a land-centric threat to a multidomain threat in which land, air and maritime domains are deeply interconnected through unmanned systems supported by cyber activity. Unmanned systems no longer refer exclusively to air platforms. There is an increasing use of maritime and land unmanned systems. This emerging combination of IEDs and unmanned systems is reshaping the threat through rapid technological evolution.

One of the key elements of the IED threat is the network associated with the device. While IEDs on the front lines will likely be employed by conventional forces, in the rear areas and European depth they will be used primarily by illicit networks of non-state actors or state-supported actors.

Countering the IED Threat

The rapidly evolving delivery vectors and the distinct environments in which IEDs may be used (in front lines and rear areas) will shape how this threat is confronted and will guide the development of a credible C-IED response.

C-IED efforts will need to be articulated, coordinated and synchronized with C-UAS, C-UGS, C-USV, C-UUV and Technical Exploitation (TE) disciplines. Artificial Intelligence (AI) and big data analytics will also be essential to manage the unprecedented volume of data expected in an Article 5 scenario.

Another key element for the C-IED response will be the triangle of responsibilities composed of the Host Nation (HN), the Troop-Contributing Nations (TCNs) and the NATO Commanders. Clearly defining the responsibilities of each within the various geographical areas of the operation will be essential to avoid gaps that could provide opportunities for the adversary.

For the purposes of this article and, considering the above as well as the C-IED pillars, two main areas of C-IED support to Article 5 operations will be distinguished:

1. Countering the IED Threat in the Front Lines

As noted, IED delivery methods will be diverse and fast-evolving. Conventional forces will be the primary users of IEDs. In this context, C-IED efforts will focus on protecting the forces, with Defeat the Device (DtD) as the leading pillar. They will need to identify and characterize the threat in order to recommend appropriate countermeasures.

Within the C-IED Understanding/Intelligence baseline, TE will serve as one of the main sources of information to support threat identification and characterization. The large-scale military formations typical of an Article 5 operation will require TE Level 2 capabilities to be pushed down to better support troops on the ground. At the operational level, efforts will focus on establishing the TE structure, organizing information and Collected Exploitable Material (CEM) flow, and managing cross-component support. In a decentralized TE structure, TE Level 2 capabilities will likely be placed at Corps level.

Attacking the Networks (AtN) will remain relevant, but the networks of interest will be at higher levels. The primary focus will be on supply chains: how various IED and unmanned system components reach

the theatre. Strategic efforts should aim to disrupt or deny the supply of these components at the highest levels of the threat networks.

2. Countering the IED Threat in the Rear Areas and European Depth

In the rear areas and European depth, the threat will differ significantly. The main responsibility to counter the threat will be on the HNs. NATO will not face a regular army, but rather an ecosystem composed of groups and networks seeking to disrupt NATO's war effort and undermine Alliance cohesion. These actors will employ IEDs alongside unmanned systems to target logistics hubs, supply routes, lines of communication, transport nodes, critical infrastructure and NATO forces and activities.

In this scenario, contributing to countering the hybrid threat through a strong interagency approach will be essential. Legal arrangements must be established to define responsibilities and mechanisms for collaboration. These responsibilities may vary from country to country, depending on national legislation and the conditions generated by the conflict.

DtD will remain important to protect the force, but in this environment, AtN will take on increased importance compared to the front lines. AtN will need to fully exploit the interagency framework. C-IED efforts will continue to engage with threat, neutral and friendly networks.

Regarding threat networks, AtN will seek to identify the links connecting the adversary's military apparatus with networks operating on European soil. Intelligence sharing between NATO and HN entities, along with TE cooperation, will be essential for identifying and targeting key nodes. Physical actions will primarily fall on the HN unless otherwise agreed. In the information environment, the objective will be to isolate threat networks from neutral and friendly networks, with a strong emphasis on security.

Conclusions

C-IED should integrate its efforts with counter-unmanned systems and TE disciplines to address emerging threats. C-IED will remain relevant in an Article 5 operation but must adapt its focus to the operational environment, whether in the front lines or the rear areas/European depth. Key enablers will include interagency cooperation, TE and technology-driven solutions, such as AI.

C-IED must become a core pillar of both NATO's overall Protection and Counter-Hybrid Threat architectures, rather than a niche enabling function.

C-IED in support to Countering-Unmanned Aircraft Systems (C-UAS)

Although C-UAS is not one of the intrinsic responsibilities of the C-IED Centre of Excellence (C-IED COE), the C-IED COE has been contributing to C-UAS from 2014, writing reports on UAS capabilities by adversary human networks, on the use of weaponized drones by them, and on C-UAS measures.

The rationale behind the C-IED COE's indirect commitment in the development of C-UAS is based on the emerging threat posed by the use of explosive-laden drones by non-state (or state-promoted) actors, which is directly related to C-IED as a whole and to Attack the Networks (AtN) and Defeat the Device (DtD) C-IED pillars in particular.

In fact, C-IED is an essential technical and analytical supporter in the field of C-UAS due to several reasons: (A) Allied C-UAS and Air Defense are not able to take care of small unmanned aircraft systems (e.g. detect or neutralize s-UASs); (B) the technical exploitation of explosive-laden drones is one of the fields of expert activity of C-IED specialists; (C) explosive-laden drones could be considered as IED-based in a high percentage of cases, and (D) the use of drones by adversary human networks is one of their capabilities to be studied and faced by C-IED (AtN).

As non-state actors are using the capabilities that unmanned aircraft system (UAS) could provide them with, UAS threat is legitimately analyzed by C-IED as a collaborative effort from Attack the Networks and Defeat the Device. Accordingly, the trends, tactics, techniques and procedures (TTP) in the use of drones by adversary human networks are falling under C-IED responsibility, as well as the technical characterization of the threats posed by their use, along with the support to technical intelligence.

Once the drone falls down from the skies, it is time to apply render-safe procedures over explosive-laden drones. Once the risk from explosive hazards is discarded, then the technical exploitation of UAS in benefit of Attack the Networks (e.g. component tracking, attribution, understanding of human network's capabilities, identification of trends, adversary TTP analysis, anticipation of own vulnerabilities, contribution to identity intelligence, support to targeting...) is clearly a C-IED responsibility.

To sum up, C-IED does not take care of the explosive-laden drones during their flight (C-UAS is responsible for that), but C-IED is working on them before they fly and once landed.

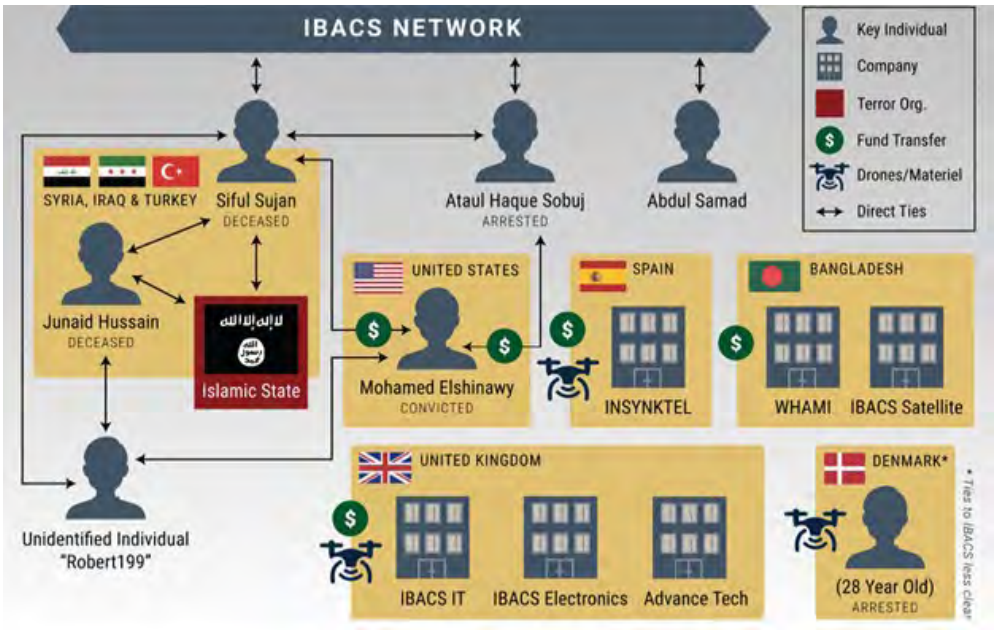


Figure 1 –DAESH-related network acquiring drone parts for Iraq & Syria (Source: www. ctc.westpoint.edu)

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"

PREPARE!

COURSES & TRAINING

Advancing WIT Capabilities in Multinational C-IED Training

Introduction: Building C-IED Expertise Through WIT Training

Each year, the Counter-IED Centre of Excellence (C-IED COE) conducts two iterations of its Weapons Intelligence Team (WIT) training course, designed to enhance NATO's exploitation capabilities in the fight against Improvised Explosive Devices (IEDs). These courses are a cornerstone in developing Level 1 C-IED Exploitation capabilities, enabling participants to collect, process and analyze battlefield Collected Exploitable Materials (CEM) when investigating IED related incidents.

WIT courses play a critical role in the broader C-IED framework. Their mission is to exploit IED incidents by gathering technical, tactical and forensic data, which feed into the intelligence cycle, further supporting NATO's C-IED Exploitation System. The course is structured to simulate real-world scenarios, ensuring that participants are prepared to operate in complex and dynamic environments.

This year's iterations of the WIT course were hosted by the Romanian Combat Support Training Center in Râmnicu Vâlcea and the Hungarian NCO Academy in Szentendre, marking another successful multinational collaboration.

Training Highlights: Râmnicu Vâlcea and Szentendre Host the WIT Iterations

The first iteration brought together 20 participants from 14 NATO and Partner nations, while the latest iteration gathered another 20 participants from 10 nations, reaffirming the multinational commitment to countering the IED threat.

For three weeks, both courses covered the C-IED Exploitation Level 1 capability, including IED components and types, forensics, photography, terrorist tactical design, s-UAS exploitation, Document and Media Exploitation (DOMEX) basic concepts and skills, post blast evidence collection and analysis. The course also included a comprehensive practical phase, during which the trainers help participants develop the skills required for future WIT operators.

"This course is more than just training: it's about building a shared understanding and operational synergy among NATO and Partner nations. Each participant leaves not only with technical and tactical skills, but also with the mindset and confidence to contribute meaningfully to the C-IED exploitation mission." - Major Georgios KRIKELIS, Instructor.

For the participating nations, this course is an excellent opportunity to understand the NATO exploitation process and to train WIT operators, enhancing their national WIT capabilities.

The course is built upon lessons learned from previous courses, incorporating updated scenarios based on feedback from operational deployments. The collaborative environment fostered knowledge exchange and interoperability among nations, a key factor in successful multinational operations.

Outcomes and Next Steps: Expanding the WIT Network

Participants successfully completed the course, demonstrating proficiency in evidence collection, scene documentation, tactical assessment and initial analysis.

Just recently, the C-IED COE has expanded its training portfolio. In accordance with the Voluntary National Contribution Fund (VNCF) agreement, a Trainers Developer Course (WIT TDC) was held at the C-IED COE in Hoyo de Manzanares, Spain, from 01 to 05 December 2025. This course aims to educate WIT Course Directors and Senior Instructors in WIT Course development by updating skills and standards and by creating WIT-related scenarios and vignettes.

In addition, the C-IED COE will host a WIT Review Workshop from 19 to 23 January 2026 at the International Demining Centre in Hoyo de Manzanares, Spain. The workshop aims to assess, synchronize and update the WIT course content to reflect evolving operational environments, technological advancements and instructional standards.

The next WIT course iterations in 2026 are scheduled for Râmnicu Vâlcea, Romania, and Szentendre, Hungary, continuing efforts to build a robust C-IED exploitation capability across Allied and Interoperability Platform nations.

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

ATNOC 2025: A Multidisciplinary and Operational Approach to Attacking Human Networks

From 17 to 28 November, the NATO-accredited Counter-IED Centre of Excellence (C-IED COE) hosted the second edition of the Attack the Networks Operational Course (ATNOC) in 2025. This two-week program, taught exclusively by subject-matter experts from the Centre, brought together 11 participants representing five NATO nations: Belgium, Hungary, Poland, Spain and Türkiye. The presence of both military personnel and civilian law enforcement professionals added significant value to the training, reflecting the comprehensive and interagency approach required to counter the Improvised Explosive Device (IED) threat and disrupt hostile human networks.

Conducted daily between 08:00 and 16:30, the ATNOC aimed to enhance the students' situational awareness and provide a multidisciplinary understanding of the Attack the Networks (AtN) approach within the broader context of C-IED. The course is designed to strengthen the students' ability to integrate and synchronize the C-IED mindset across headquarters processes, ensuring coherence and coordination among different staff functions and partner agencies.

The course is structured around four key phases that define the AtN work cycle: **FRAMEWORK, HUMAN NETWORKS, ENGAGEMENT and ASSESSMENT.** The Framework phase lays the foundation by examining the threat environment, operational variables and systemic understanding of the adversary. This conceptual groundwork is essential for guiding a coherent and effective AtN approach throughout the rest of the course.

The second phase, Human Networks, focuses on identifying and analyzing hostile networks. Students are introduced to advanced analytical methodologies, network typologies, behavioural patterns and social dynamics. By understanding the structure and functioning of these networks, participants learn to identify critical nodes, vulnerabilities and opportunities for engagement.

The Engagement block constitutes one of the most operationally oriented components of the course. It introduces both lethal and non-lethal options for engaging with and disrupting hostile networks, combining traditional military capabilities with civilian, informational and interagency tools. This comprehensive approach underscores the need for coordinated action across military and non-military domains to achieve lasting operational effects.

The final block, Assessment, teaches students how to evaluate the impact and effectiveness of their actions. Using assessment models, performance indicators and feedback mechanisms, participants learn to measure the outcomes of engagements and understand their contribution to reducing the IED threat in complex operational environments.

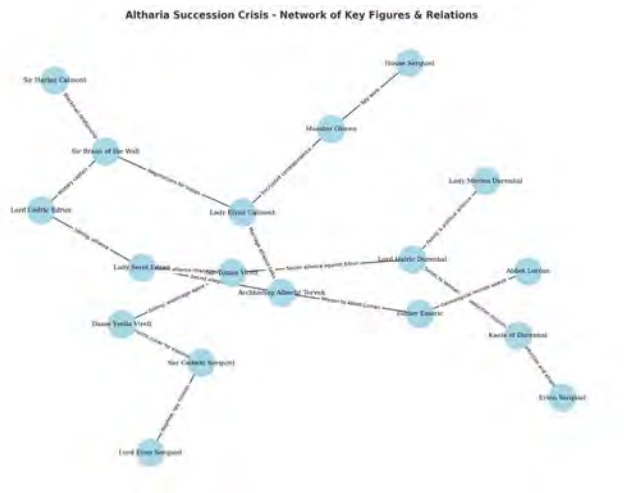
The teaching methodology of this edition combined theoretical instruction with extensive practical work. After each conceptual block, students were assigned to working groups where they applied what they had learned using a realistic and current scenario based on the security situation in Mali. This hands-on component allowed the participants to execute the full AtN cycle, from network analysis and operational planning to engagement recommendations and post-action assessment.

The performance of the students exceeded expectations. Throughout the course, the working groups produced high-quality analytical products, operational proposals and assessments that were highly valued by the course staff and instructors. The mix of military and law enforcement backgrounds proved to be a significant asset, demonstrating the importance of cross-functional and interagency collaboration when confronting the evolving IED threat.

The instructors, experienced specialists from the C-IED COE, provided expert guidance supported by lessons learned from NATO missions and Allied

operational deployments. Their diverse backgrounds enriched the training and ensured a realistic, relevant and comprehensive approach to the subject matter.

The 2025 ATNOC has once again established itself as a key training opportunity within the NATO C-IED community. Its multidisciplinary structure, technical precision and operational focus make it particularly suitable for military personnel and law enforcement officers working in intelligence, operations, plans, targeting, C-IED, CIMIC and information activities. This edition reinforces the importance of preparing professionals capable of addressing complex threats and disrupting hostile networks in today's operational environments.



Support to NATO SP COE on a Mobile Training Solution (MTS) on Battlefield Evidence (BE) Course for Ukrainian Participants

In support of Military Cooperation and Capacity Building and at the request of SHAPE, NATO Stability Policing Centre of Excellence (NSP COE), together with the C-IED COE and other forensic and law enforcement experts, deployed a Mobile Training Team (MTT) on Battlefield Evidence (BE) to the Joint Force Training Centre (JFTC) in Bydgoszcz, Poland, for Ukrainian participants primarily representing national investigative bodies — both military and civilian.

The aim of this initiative was to provide tactical commanders operating in deployed environments with essential forensic knowledge and skills, enabling them to properly collect, preserve and document information and materials obtained in battlefield conditions.

The pilot course took place from 13 to 17 October 2025, under the lead of NSP COE. As part of this collaborative effort, the C-IED COE contributed with two subject matter experts (SMEs) who delivered lectures and practical demonstrations on basic Weapons Intelligence Team (WIT) procedures, complemented by hands-on training using WIT equipment and techniques.

This engagement reinforced the shared commitment of participating organizations to enhance operational

readiness and ensure the proper handling of potential evidence collected during military operations.

What is Battlefield Evidence?

Battlefield Evidence (BE) refers to any information or material obtained during NATO operations, missions or activities that may subsequently support law enforcement and judicial processes.

BE can then be shared or transferred to Allies, Partners, Non-NATO Entities (NNEs) and/or Host Nations (HNs) to contribute to broader security and accountability objectives.

The sources of BE can be diverse, encompassing collected exploitable materials (CEM), biometric data, intelligence products, imagery and other outputs of military activity. Moreover, operational records or documentation generated by NATO forces may also constitute BE, when relevant to investigations or prosecutions.

By properly managing BE, military forces can help bridge the gap between operational success and legal accountability — ensuring that actions taken in the field can support justice and long-term stability.

Strengthening Cooperation Between "Green & Blue"

The effective use of BE relies on close cooperation

between the military ("Green") and law enforcement agencies ("Blue"). Both communities play distinct but complementary roles in the BE process.

From a military perspective, BE serves intelligence purposes by supporting information collection and analysis for operational decision-making, assists in accurate targeting, and enhances force protection by defining threats and identifying tactics, techniques and procedures. Military personnel on operations are responsible for securing the battlefield, identifying, marking and documenting evidence locations, collecting and preliminarily analysing physical evidence, maintaining the chain of custody, and preventing contamination or alteration of materials. They must also ensure prompt reporting to military headquarters or designated liaison officers.

Law enforcement agencies, on the other hand, are responsible for ensuring that the materials collected on the battlefield are suitable for judicial use. They receive evidence from military authorities while maintaining the integrity of the chain of custody, conduct detailed forensic analyses, and record and store all items in accordance with national and international legal standards. Their role also includes preparing evidence for court proceedings or further investigation and coordinating with military and judicial authorities to ensure verification and transparency.

This complementary relationship ensures that materials gathered in operational environments can be lawfully used in judicial processes, reinforcing accountability and adherence to international norms.

Conclusion

The joint effort between the C-IED COE, NSP COE and the entities involved in providing this Mobile Training Solution on Battlefield Evidence marks a significant step toward enhancing interoperability and shared understanding between military and law enforcement professionals.

Through this pilot course for Ukrainian participants, the value of joint training, cooperation and mutual support became evident in order to address the complex challenges of modern conflict environments, where the collection and preservation of Battlefield Evidence is not only an operational necessity, but also a key element in ensuring justice and legitimacy.

This initiative demonstrates NATO's commitment to fostering resilience, legality and interoperability across operational domains.

Counter-IED Centre of Excellence Support to Collective Training in 2025

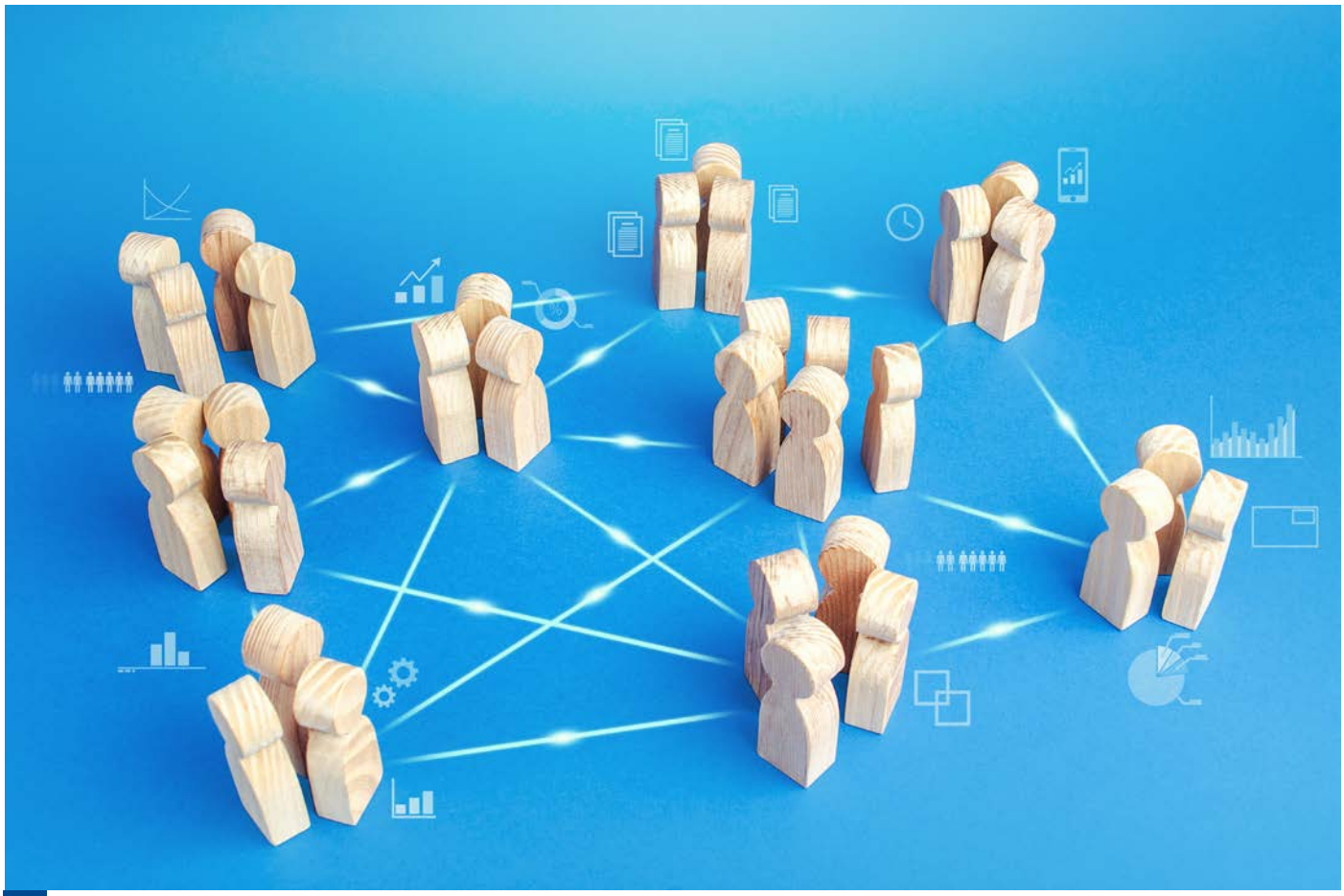
Throughout 2025, the NATO Counter-Improvised Explosive Devices Centre of Excellence (C-IED COE) contributed to Allied collective training and national capability development, complementing its delivery of specialized individual education courses. Embedded across Supreme Allied Commander Europe's Multi-Year Training and Exercise Programme (MTEP), the Centre's activities enhanced interoperability, multi-domain operational readiness, and counter-IED competence in response to evolving threat trends.

As part of its support to ACT and maritime experimentation, the C-IED COE contributed to Dynamic Messenger 25 in Portugal under the NATO Maritime Unmanned Systems (MUS) Initiative. The exercise enabled operational testing of unmanned platforms in reconnaissance, seabed monitoring, and threat detection, with the Centre assessing their application in exploitation and mitigation tasks in littoral environments.

In the land-focused joint context, Loyal Leda 25, hosted at the Joint Force Training Centre (Bydgoszcz, Poland) integrated counter-IED into an Article 5 command-post operation. Subject-matter experts reinforced intelligence fusion, force protection and counter-threat synchronization across dispersed formations.

The Centre also supported Northern Challenge 25 in Iceland, one of Europe's longest-running improvised explosive device disposal exercises. Participants conducted land and maritime disposal tasks under NATO Defense Against Terrorism (DAT) sponsorship, supported by a multinational exploitation coordination cell, level 2 laboratory, and dedicated intelligence elements.

At the operational level, the Maritime Security Exercise (MARSEC) 25 in Türkiye strengthened maritime situational awareness and inter-agency coordination among NATO, EU and partner nations. The C-IED COE provided specialist input on counter-threat networks



in complex maritime frameworks.

Within the multi-domain environment, Steadfast Duel 25 (STDU25) in Stavanger, Norway, tested NATO Command Structure (NCS) headquarters against peer adversaries and hybrid threat actors as part of the re-curring STEADFAST series. The exercise incorporated cyber, space and information-environment dynamics, with the Centre supporting exploitation-driven target-ing and cross-domain synchronization.

At the tactical level, Loyal Dolos 25 (LODO25) trained NATO Rapid Deployable Corps Greece in the execu-tion of land-focused offensive operations. The C-IED COE emphasized route-clearance considerations and manoeuver risk assessment during tempo-based planning.

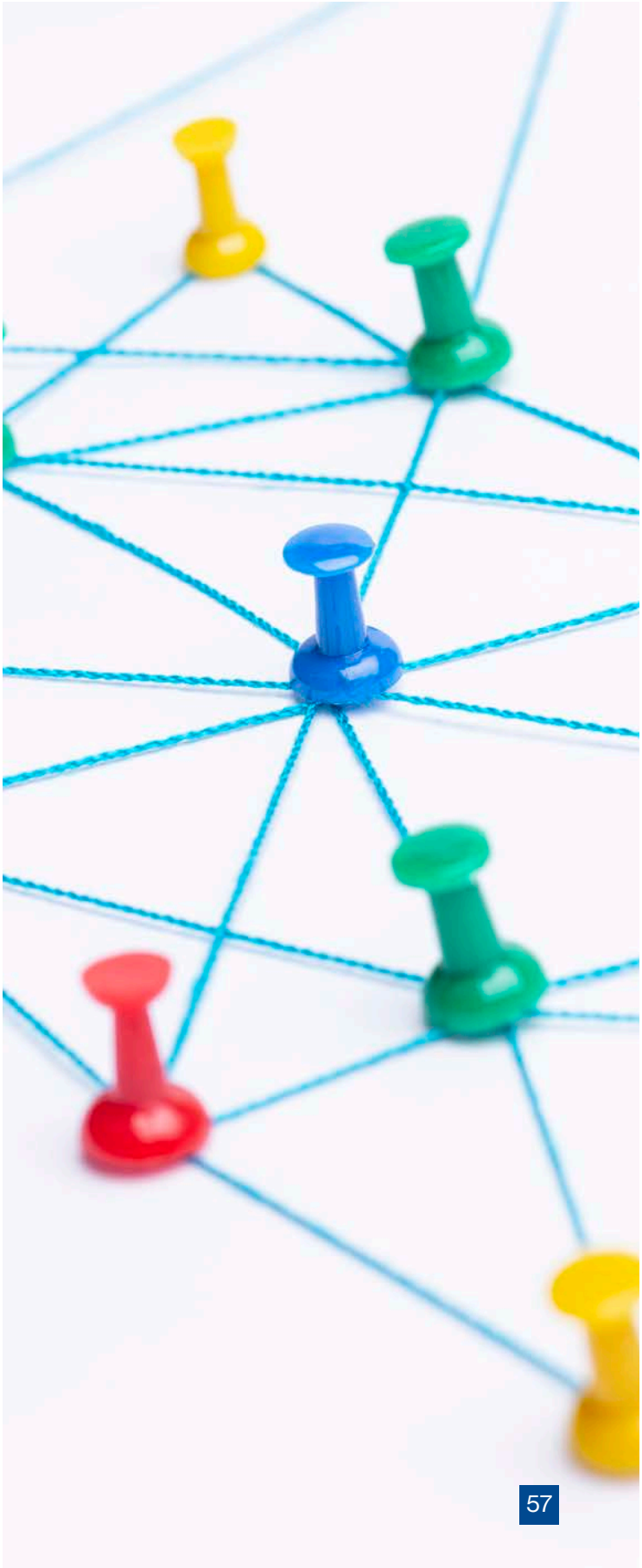
NATO's readiness oversight continued through Combat Readiness Evaluations (CREVAL) for Rapid Deployable Corps in Greece and Spain under Allied Land Command (LANDCOM) leadership. These assessments measured crisis response planning, command-and-control agility and sustainment, with the Spanish evaluation linked to the upcoming LOLE26 exercise.

Finally, Valiant Blaster 25 (VABL25), hosted by Spain's Tercio de Armada, was conducted as a seminar for-mat this year. With the participation of the C-IED COE subject-matter experts, the event reinforced doctrinal alignment, technical exchange and exploitation-linked targeting, responding to emerging challenges such as unmanned systems and homemade explosive precursors.

Across 2025, the C-IED COE played a central role in strengthening Alliance preparedness. By supporting MTEP-aligned collective training and embedding counter-IED considerations in planning and execution, the Centre contributed to NATO's broader deterrence and defense posture.

As for the incoming 2026, the Centre plans to main-tain the level of support, increasing the coordination with Training audiences and EXCON actors, as well as improving the integration of C-IED aspects, from Technical Exploitation at Tactical level to the Opera-tional and Strategic level staff processes.

The C-IED discipline is not limited to any specific level of command, single service domain or type of military operation. The continuously evolving threat posed by improvised explosive devices, whether emplaced on land, flown or deployed at sea, is forcing realistic training scenarios to adopt a level of dynamism hardly seen before.



DOMEX New Structure
Two Phases, One Mission: Crafting the Next Generation of Battlefield Exploiters

Abstract

Technical Exploitation has become an essential enabler for commanders conducting Multi-domain operations against adaptive and networked threat organizations. Through the rapid collection, processing and analysis of collected exploitable material, Technical Exploitation produces actionable intelligence that illuminates enemy networks, accelerates targeting and supports decision superiority at every echelon.

Document and Media Exploitation (DOMEX) is a fundamental pillar of Technical Exploitation, enabling the transformation of captured documents and digital data and metadata into operational intelligence. In an era where NATO forces face increasingly complex, data-rich and technologically adaptive adversaries across new operational scenarios, the role of DOMEX has become even more critical.

This article explores the advantages Technical Exploitation provides to commanders and deployed forces, outlines the unique considerations inherent to DOMEX, and introduces the enhanced three-week DOMEX Course. The updated course curriculum has been structured into two sequential phases, Operator and Analyst, providing the attendees with the skills required to acquire, process and analyze information, data and metadata within a modern exploitation framework aligned with current and future NATO operational demands.

The Operational Benefits of Technical Exploitation

In intelligence usage, NATO defines Technical Exploitation (TE) as a process of applying scientific methods and tools to derive results of value from collected exploitable material (CEM). TE provides commanders with a decisive advantage by converting CEM into actionable intelligence, uncovering enemy intent, capabilities and network structures. Key benefits include:

- **Actionable intelligence**: By enabling quick triage and exploitation of CEM, transforming raw data into actionable insight and allowing commanders and analysts to use fresh information and data before adversaries can adapt. This enhanced intelligence production allows commanders to identify critical nodes, facilitators and functions within threat networks, while also exposing their financial, logistical and communication pathways, thereby improving the accuracy of targeting. Because TE draws directly from unfiltered digital or physical evidence, its outputs often provide higher-fidelity insight than traditional reporting, offering precise geolocation data, communication patterns, timelines and robust corroboration of HUMINT, SIGINT or other operational information.

- **Force protection:** By contributing to preventing attacks through early warning of enemy plans, emerging technological adaptations and Tactics, Techniques and Procedures (TTPs) to light.

- **Legal Prosecution:** Outputs can be used as evidence in criminal prosecution. The chain of custody procedures and forensic analysis ensure materials meet evidentiary standards which facilitate the cross-agency and international collaboration, supporting prosecutions processes and international sanctions.

Collectively, these contributions enhance predictive awareness, support risk assessment and route planning, and enable commanders to achieve decision superiority in dynamic operational environments.

Specific Considerations for DOMEX

DOMEX is a core sub-discipline of TE that focuses on the systematic capture, process, translation and analysis of information from collected documents and media, both physical and digital. Modern conflict zones are populated with documents and digital media: every phone, tablet, drone controller or flash memory may hold vital clues about enemy intentions, logistics or external support.

Recent operational trends demonstrate that DOMEX has become an outstanding capability, offering critical insights that support decision-making, targeting and long-term operational/strategic planning. Several aspects make DOMEX unique:

- **Network identification and disruption across multiple domains.** By exploiting contact lists, communications, financial records and media files, DOMEX can uncover motivation and ideology, financial networks, logistics chains, hidden relationships, enemy capabilities, travel patterns and organizational and command structures. This network analysis will be essential for targeting operations, Counter-IED operations, counterintelligence, and disrupting enemy operations, which provides strategic, operational and tactical insight at the same time:

- Strategic: ideology, external support, international leadership.

- Operational: network structure, supply chain, finance.

- Tactical: immediate threat information, locations, timetables.

- **High data volume, variability and complexity.** Modern digital devices generate enormous quantities of data, including multiple file systems and encryption schemes, redundant, hidden or deleted data, diverse formats across mobile, computer, Unmanned Systems and removable media and multiple languages. This requires specialized training, disciplined workflows and validated forensic tools.

- **Time Sensitivity and Specific Data Exploitation.** Captured digital media can degrade quickly through environmental exposure or deliberate tampering, so DOMEX operators must conduct rapid tactical extraction on-site or in austere conditions, work with partial or damaged media and prioritize data categories based on operational need.

- **Forensic Integrity.** DOMEX outputs may support target development, threat assessments or judicial processes, so maintaining forensic integrity by using standardized acquisition protocols, cryptographic hashing and verification and detailed reporting and documentation, is critical.

- **Blends Physical and Digital Exploitation.** Most TE disciplines are physical (weapons, material) or digital (cyber), but DOMEX is one of the few that comprises both. For example, a handwritten letter found in a safe house, a laptop drive image containing encrypted files, a photo showing members of a network together or metadata from an unmanned aerial vehicle (UAV). This hybrid nature makes it uniquely adaptable across environments and domains.

- **Requires Linguistic, Cultural, and Behavioral Interpretation.** While other TE processes are primarily technical or forensic, DOMEX requires translation, language pattern analysis, cultural understanding and human behavior assessment to extract the maximum information from the collected material.

DOMEX has proven especially effective in uncovering hybrid threats, where state-backed private military companies (PMCs) and non-state violent extremist organizations (VEOs) collaborate in grey-zone operations. In these environments, the exploitation of cap-

tured media provides unique windows into adversarial intent that may not be accessible through traditional Intelligence, Surveillance and Reconnaissance (ISR).

The New Three-Week DOMEX Course Structure

Recognizing the important role of DOMEX in current operations, the Counter-Improvised Explosive Devices Centre of Excellence (C-IED COE) has been training NATO personnel in the DOMEX field, since 2019, through a training package comprised by a basic and an advanced course. In 2024, NATO started to directly support the DOMEX training, enhancing the remarkable outcomes and strengthening the international interest in the project.

DOMEX training continually evolves, integrating valuable feedback from instructors and attendees, along with insights from real-life experiences, to enhance the training programme and meet the demands of the modern battlefield. This ensures that attendees are equipped to address emerging challenges with up-to-date expertise.

To accommodate the increasing operational demand and technological complexity, the prior two-week DOMEX Course has been rebuilt into a more exhaustive three-week programme, including both basic and advanced DOMEX content. The new structure differentiates between Operator-level and Analyst-level inside DOMEX, giving a more consistent learning track.

The course is designed for trained International or National Field Exploitation Team (FET), Weapons Intelligence Team (WIT), or equivalent specialists, and is conducted multiple times annually. The aim is to provide essential Technical Exploitation training, at basic and advanced level, focused on:

- Document Exploitation (DOCEX)
- Media Exploitation (MEDEX)
- Cellular Phone Exploitation (CELLEX)
- Unmanned Systems (UxS) Exploitation

For the most recent schedule and to register, please visit the C-IED COE official website (www.ciedcoe.org).

The current course structure is comprised of two independent but complementary phases, as follows:

Phase I: DOMEX Operator (Weeks 1–2)

This phase trains attendees to conduct the technical collection and initial exploitation of digital media. Regarding DOCEX, MEDEX, CELLEX and UxS Exploitation, emphasis is placed on:

- CEM search, collection, identification and processing.
- Forensic acquisition of mobile devices, computers and removable media.
- Use of digital forensics tools for extraction.
- Imaging procedures and verification using cryptographic hashes.

- Proper documentation, labeling and chain-of-custody protocols.

The graduates from this phase will be able to:

- Preserve physically the CEM and the data and metadata included in it.
- Conduct safe, forensically sound acquisition of mobile, computer media and Unmanned Systems data and metadata.
- Extract priority data categories based on mission requirements.
- Deliver live extraction procedures when needed.
- Maintain complete forensic documentation, including hashes and logs.
- Apply metadata understanding to provide context during rapid exploitation.
- Extract data from a damaged electronic device (by Chip-Off).

Phase II: DOMEX Analyst (Week 3)

This phase trains analysts to sort out the extracted data and produce actionable outputs for intelligence, force protection and legal purposes. Training includes:

- Data and metadata interpretation.
- Deep-dive analysis using a number of digital forensics tools.
- Reconstruction of user activity, timelines, communications and file interactions.
- Identification of hidden, deleted or obfuscated data.
- Link analysis and network mapping.
- Production of detailed exploitation reports for targeting and operational planning.

The graduates from this phase will be able to:

- Build analytical narratives from raw extracted data.
- Search for specific information found in the acquired forensic images.
- Identify relationships, networks and indicators of threat activity.
- Perform advanced searches, timeline creation and artifact reconstruction.
- Generate initial extraction reports to support analysts and commanders.

Personnel interested in this training may choose to attend only the phase that aligns with their specific professional role. However, attending both phases is strongly recommended, as it provides a comprehensive understanding of the entire exploitation process and enables participants to achieve excellence in the DOMEX field.

Conclusion

The evolution of Technical Exploitation, and DOMEX in particular, reflects the evolving realities of modern, data-dense conflict environments where rapid, precise intelligence is essential for operational success. As adversaries adopt increasingly complex technologies and disperse their networks across physical and digital domains, the ability to convert captured material into actionable insight becomes a decisive advantage.

DOMEX ensures that commanders at every echelon can respond faster, target more accurately, and operate with greater decision superiority.

The redesigned three-week DOMEX Course directly supports this operational imperative, equipping both operators and analysts with synchronized skill sets tailored to NATO's current and emerging mission demands. By dividing training into Operator and Analyst phases, the programme strengthens the full exploitation workflow, from the preservation and acquisition of sensitive data in any conditions to the deep analytical processes that uncover enemy intent and structure.

Together, these phases cultivate a new generation of battlefield exploiters who are prepared to meet the challenges of hybrid threats, high-volume digital environments, and rapidly evolving technologies, ensuring DOMEX remains a cornerstone capability for Multi-domain operations.

tadaweb

OPERATING SYSTEM FOR OSINT

POWERED BY AI

ACCELERATE USER EFFICIENCY AND EFFECTIVENESS

Seamlessly pivot between Secure Browse, Investigate, and Monitor.

Reduce analysts' burnout, improve knowledge retention, and boost effectiveness.

STAY AGILE IN A DYNAMIC OSINT LANDSCAPE

Boost analysis and reduce strain for sharper OSINT insights. Versatile platform for diverse use cases.

Easily integrate 3rd party tools and APIs.

MAINTAIN COMPLIANCE WITHOUT COMPROMISING ANALYSIS

Manage user activity, from data access to security. Meet retention standards with custom auto-export and deletion.

Audit logs ensure transparency and quality.

© 2025 Tadaweb S.A. / Tadaweb Technologies USA Inc.
The photo used on this ad is AI-generated / ES-2025 11

Learn more and book a demo today at

tadaweb.com/bookademo

ADDING C-IED AND TE PERSPECTIVE

CONFERENCES, SEMINARS AND WORKING GROUPS

C-IED and Technical Exploitation Annual Conference 2026

"The Evolution of Counter-IED Operations: Expanding the Threat Horizon"
15–18 June 2026 | Valencia, Spain

The C-IED COE will host its Annual Conference on Counter-IED and Technical Exploitation (TE) from 15 to 18 June 2026 in Valencia, Spain.
The 2026 edition, under the theme "The Evolution of Counter-IED Operations: Expanding the Threat Horizon," will gather representatives from NATO entities, Partner Nations, international organizations, industry, law enforcement and academia.

This annual event serves as a key forum for collaboration, innovation and knowledge exchange across the global C-IED and Technical Exploitation communities. It provides an opportunity to address NATO's evolving challenges, share operational experiences, identify capability gaps, and explore practical solutions.

Building upon the success of previous conferences, the 2026 edition will feature an opening day dedicated to plenary discussions, followed by focused breakout sessions over the next two days, fostering cross-disciplinary engagement across five core areas:

- C-IED Support Across Military Operations: Examining the integration of C-IED and TE capabilities across the full spectrum of operations, from low-intensity conflicts to large-scale warfare.
- Advancing NATO's Technical Exploitation Capabilities: Promoting cooperation and development of TE initiatives among NATO Allies, Partner Nations, law enforcement, and industry stakeholders.
- Information and Intelligence Sharing: Facilitating the exchange of threat information on ongoing conflicts, emerging technologies and developments in C-IED and TE training, education and equipping.
- Lessons Learned and Community Insights: Bringing together experts to share operational experiences, highlight best practices and discuss evolving requirements in C-IED, TE and Battlefield Forensics.
- Innovation and Enablers: Strengthening collaboration with industry and academia to support NATO's defence planning priorities for capability development, experimentation and conceptual design.

For further information or coordination, please contact: ciedac@ciedcoe.org

Mobile Training Team in Georgia

From 22 to 25 September, the C-IED COE organized a Mobile Training Team (MTT) for Georgian Defence Forces. The activity took place in the Georgian Army Engineer School near Tbilisi, the capital of Georgia.

The training was part of the NATO PfP programme and was focused on introducing C-IED to Georgian Defence Forces representatives. The introductory programme had a diverse audience, formed by officers and NCOs with various assignments, spanning from Battalion to General Staff.

The 4-day training was intended to give an initial, yet consistent introduction about what is C-IED within NATO and how it is developed.

The Georgian Military representatives have shown interest in a future cooperation on this matter, with the intention to develop a national C-IED military capability, so two different courses of action will be carried out. First, a series of future MTTs will be deployed in Georgia; and second, some of the C-IED courses will be open to Georgian students.

This is a perfect example of successful cooperation, not only from NATO PfP perspective, but also as a Defence Capacity Building activity which means a starting point for further collaborative efforts with the Georgian Defence Forces and the declared intention to build a Georgian national C-IED capability.

Current Situation of C-IED in Africa

A year ago, we wrote an article about the situation that many African countries suffer with a big IED threat in extensive parts of their countries and how those countries started to need a broader C-IED training beyond the traditional device centric, tactical level one. In that article we also described what could NATO do, and specifically what the C-IED COE could do to help them in that path.

During this year, the C-IED COE has continued attending several forums and introducing some initiatives, giving continuation to the work done in the past years. We continued developing a possible support to Tunisia to help them broaden their curriculum in their outstanding Centre of Excellence, so they can also teach their armed forces and other armed forces of the region, with courses beyond the tactical level.

We also finished the planning of a project with Jordan that will mean the deployment of a Mobile Training Team (MTT) to teach a C-IED Staff Officer Course, similar to the one we hold at the C-IED COE, but tailored to their needs. This cooperation will probably last until they have the capacity to continue their training by themselves, after three or four deployments of this MTT.

Furthermore, regarding the possible cooperation with nations or organizations, we continued the support to United Nations, specifically with UNMMAS, exploring ways in which the C-IED COE could support them in better preparing nations and contingents in C-IED. This cooperation has had a tangible result in helping them rearrange their EOD courses and requirements in the IEDD area.

In spite of our efforts to expand their curriculum in the Entebbe (Uganda) training center, we regret to say that the development has not been as productive as we had expected, due to several reasons.

We also continued to support the Global Counter Terrorism Forum (GCTF) in their West Africa Working Group project, witnessing the finalization of the so-called Lomé Recommendations, a document meant to be a master set of recommendations for countries and regional organizations on how to deal with the C-IED threat.

These recommendations cover all aspects, from political requisites to judicial ways of acting; from international cooperation requirements to population education and awareness; and thanks to the C-IED COE participation in the project, it also includes critical aspects to disrupt the networks, such as military requirements, interagency approach, precursors control, etc.

Finally, we attended this year iteration of the African C-IED Annual Conference, the 7th one, witnessing how, in one year, the scope of C-IED capabilities and training of the African nations and organizations has been steadily growing in the correct direction. Among the briefings presented, there were several that, in our opinion, show serious advances in proper C-IED capability development.

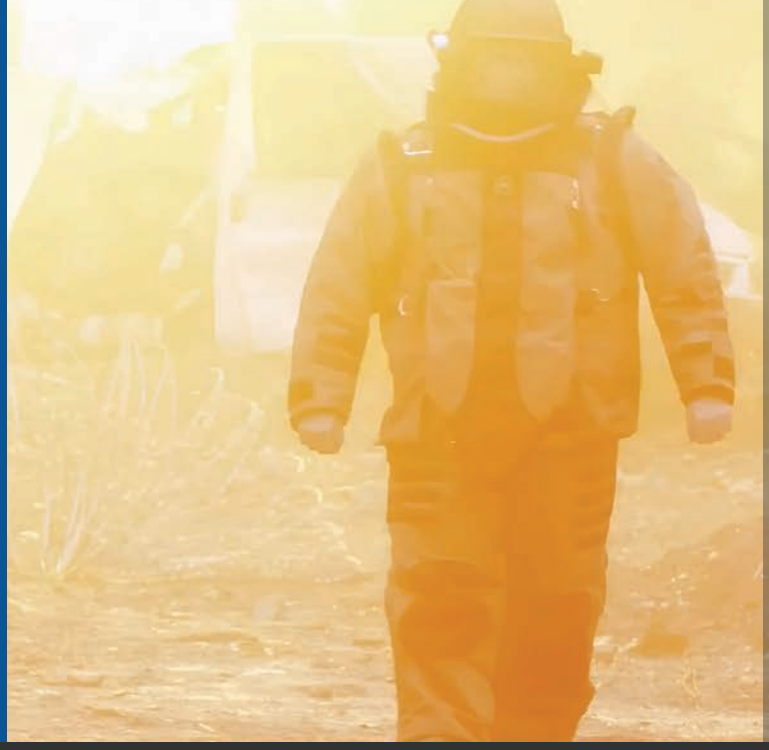
The first one is the African Union briefing about their draft C-IED Strategy. Although the approach is completely different to NATO'S, it is interesting to see how they tick all the important boxes and they produce a perfectly usable policy. Of course, it is still a draft, although apparently in a very advanced stage, and there is a long way ahead until it is implemented by nations of the AU, but it is definitely a very good policy that could make a difference.

The briefing from the AUSSOM (African Union Support and Stabilization Mission in Somalia) was also very interesting and a good example of a properly conducted operation, specially together with the presentation of the Somali C-IED strategy for the next five years.

We would also like to mention a Kenian representative from their Strategy and Defence Headquarters, who presented their process for developing their own Policy and Strategy, making it a very good example of what can be done with the proper initiative, support and understanding of the problem.

To sum up, the situation of the C-IED discipline in Africa is far from being satisfactory, but signs show that they are going in the right direction and NATO can definitely support and help speed up the process.

ALFORD



INNOVATIVE EXPLOSIVE TOOLS TRAINING R&D

www.explosives.net

A comprehensive range of cutting-edge charges and disruptors to counter IED & VBIED threats.

Highly reliable, proven, and patented technologies trusted by military and security forces worldwide.

IEDD TOOLS

IEDD courses are based on NATO SOPs and other international requirements, from basic to advanced operator standards.

HME courses follow the latest terrorist threats.
All courses bespoke to the customer and the threats they face.

IEDD & HME TRAINING

Renowned for our innovative R&D capabilities, we are firmly established as a world leader in explosive tools.

We combine scientific expertise with operational experience to develop cutting-edge solutions.

R&D

Soldier in the Spotlight

Col. Javier Sanz (ESP A), C-IED COE Director

The Counter-Improvised Explosive Devices Centre of Excellence (C-IED COE) has a new Director at its helm. As the threat landscape evolves, we sat down with the Director to discuss his background, vision for the Centre, and the future of C-IED efforts within NATO and beyond.

Q: Director, welcome! Thank you for taking the time to speak with us. To start, could you tell us a bit about your professional background and what experiences have shaped your approach to C-IED?

A: Thank you. It is a pleasure to be here. During my military career I have been in contact with C-IED matters as an Engineer Officer, as I have been mainly focused on posts linked to the Engineering Branch. Prior to this appointment, I have had the opportunity to command an Engineer Regiment as a Colonel, where I had the chance to be the Exercise Control Director of the largest C-IED exercise hosted by Spain under the umbrella of the European Defense Agency, Bison Counter 25.

On the other hand, I am also a General Staff Officer and this has put me in contact with the interagency and interdisciplinary nature of C-IED activities, especially on operations and in international environments. These experiences instilled in me the importance of a multi-faceted approach: integrating intelligence, technology, operational expertise and strong partnerships.

Q: Congratulations on your appointment as Director. What was your reaction when you learned you had been selected to lead the C-IED COE?

A: I was deeply honored and humbled. The C-IED COE is a globally recognized institution that plays a vital role in protecting our forces and civilian population. I also felt a strong sense of responsibility to build upon the excellent work of my predecessor, Colonel Corbacho, and all those who have contributed to the Centre's success since 2010.

Q: What do you see as the primary role of the Director, and what are your immediate priorities as you take command?

A: The Director is responsible for the overall day-to-day management of the C-IED COE, encompassing programme and budget oversight, as well as the direction of C-IED COE personnel from both Sponsoring Nations and the Framework Nation. For these tasks, I rely on the support of my dedicated staff and administrative branch to ensure smooth operations.

However, my primary responsibility centers on the Programme of Work (POW) and fostering strong relationships with NATO, as our primary customer, and other external organizations and partners who can benefit from our expertise.

My immediate priorities are threefold: first, to gain a comprehensive understanding of the current capabilities and ongoing projects within the COE; second, to strengthen existing partnerships with our Participating Nations and key stakeholders; and third, to strategically assess how we can evolve to address emerging threats and effectively support NATO's evolving priorities.

Q: You mentioned evolving threats. How do you intend to strengthen the links between military and civilian personnel to provide relevant solutions to emergent explosive threats?

A: Our strength lies in the interagency nature of the C-IED COE. Military and civilian personnel, security forces, intelligence services and academia work together every day with one common goal: reducing the threat and saving lives. My intention is to further strengthen these working links to provide relevant solutions to the emergent explosive threats, highlighted by the current conflicts in Ukraine, Gaza and the Sahel, as well as in other places, where terrorist networks exert influence.

Q: What new challenges are you seeing in the C-IED landscape, and how is the COE adapting to meet them?

A: The threat of IEDs has evolved with the integration of emerging technologies like drones, 3D printing and commercially available electronics, making them more sophisticated, harder to detect, and easier to deploy remotely. This adaptability, along with new ways of hiding and triggering them, means that we must keep constantly improving how to detect them, sharing intelligence and coming up with updated countermeasures.

Q: Looking ahead, what are some possible paths for the future mission of the C-IED COE? We understand there is discussion about expanding the scope.

A: That is correct. Since its accreditation in 2010, the C-IED COE has been a unique instrument in NATO's toolbox. It is time to evolve and remain relevant, providing cutting-edge tools to the international community, to enable it to remain strong against the scourge of improvised explosive threats.

One area we are exploring is the integration or expansion of complementary activities, such as Technical Exploitation and Battlefield Evidence. We are considering a change that would better reflect the broader spectrum of threats and the expanded skillset encompassed within the Centre, becoming the Counter-Improvised Explosive Systems and Battlefield Forensics Centre of Excellence.

The Centre must be ready to adapt its structure and activities to keep on meeting the Alliance command objectives and to be aligned with NATO strategic priorities for 2030. The C-IED COE will thus remain a relevant source of knowledge and practical resources for NATO's transformation and Multi-domain operations, where C-IED support and capabilities are integrated within all domains and able to operate in them simultaneously, delivering effects in the virtual, cognitive and physical dimensions.

Q: How is the C-IED COE's work contributing to the security of Allied and Partner nations?

A: In the past, we have helped reduce casualties, protect freedom of movement and strengthen multinational interoperability in asymmetric environments by supporting operations.

But the type of threat once centered almost exclusively on land-based IEDs has now evolved into new, more complex manifestations across the physical domains: unmanned systems carrying explosives, improvised weapon systems built with commercial components, or hybrid networks blending criminal, insurgent and state-backed actors. With our updated work, we hope to continue providing a helpful contribution against these threats.

In order to achieve this, one of the Director's enduring priorities is to ensure that every Steering Committee member fully understands that the COE is their Centre: we are an institution that exists to support the collective interests of all Sponsoring Nations. We take every RFI and RFS very seriously, and for that reason we are strengthening the role of Senior National Representatives as genuine interlocutors with their respective nations.

Their ability to clearly articulate national priorities is essential for us to provide the level of support expected from a Centre in which they are directly represented. For example, during the most recent Steering Committee, members were reminded that the Centre stands ready to support national exercises, offering an ideal opportunity to train, validate and enhance C-IED capabilities.

Q: What is the main message you wish to convey to the staff as you present your Guidance for 2026?

A: My first message is very clear: professionalism, ethics and relevance must be the foundation of everything we do. The operational environment is changing rapidly, shaped by hybrid threats, disruptive technologies and NATO's shift toward Multi-domain operations.

To remain the leading global hub for expertise on IED systems, each member of the Centre must stay informed, curious and committed to excellence. That means basing our assessments on facts, strengthening both internal and external communication, and ensuring that our work consistently reflects the high standards expected from an international military organization. Our credibility starts with how we think, how we act, and how we represent the Centre every day.

Q: And what priorities do you expect the staff to focus on as the Centre heads towards 2026?

A: I expect initiative, innovation and unity of effort. Every individual contribution matters, and I encourage our staff to be proactive, to think creatively, and to make full use of their expertise. This year, we must reinforce our relevance by integrating C-IED considerations into NATO exercises, strengthening cooperation with Partners and law enforcement agencies, and advancing new capabilities in Technical Exploitation and Battlefield Evidence.

At the same time, we must enhance internal cohesion: through better communication, training and teamwork. Ultimately, if we align our actions with our mission and strategic objectives, we will ensure that the Centre continues to evolve effectively and remains a trusted, indispensable actor within NATO and the international community.

Q: Director, thank you for your insights. Any final thoughts you'd like to share with our readers?

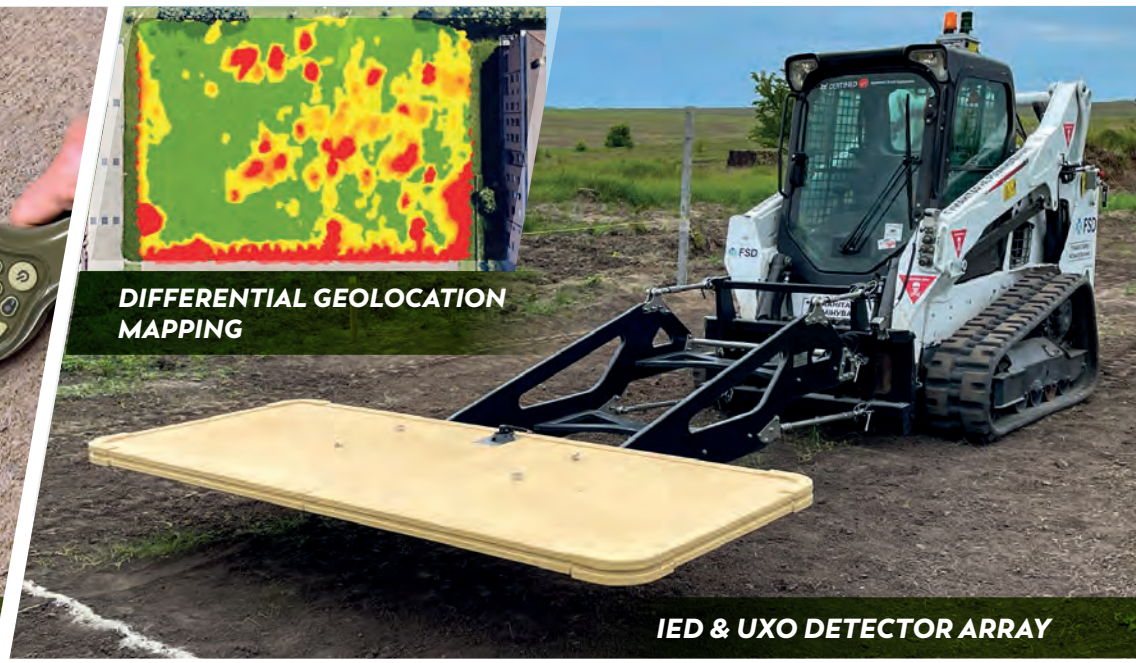
A: I recognize the significant challenges and responsibilities inherent to this role, and I am committed to leading with integrity, transparency and an unwavering commitment to our core values. This is an exciting opportunity to shape the future of C-IED efforts and contribute to the safety and security of our forces and Allies.

I firmly believe that, together, we are more than capable of overcoming any obstacle, adapting to emerging threats and excelling in everything we do. I encourage everyone to continue to share their ideas and concerns, as collaboration is essential to our success.

THREAT DETECTION THROUGH MULTI-SENSING TECHNOLOGY

- **MD** COMPACT METAL DETECTOR
- **GPR** GROUND PENETRATING RADAR
- **CRD** CARBON ROD DETECTOR
- **WD** COMMAND WIRE DETECTOR

URBAN CLEARANCE



DIFFERENTIAL GEOLOCATION MAPPING

IED & UXO DETECTOR ARRAY

CEIA • Zona Industriale 54, 52041 Viciomaggio - Arezzo (ITALY)
+39 0575 4181 • infogsmd@ceia-spa.com

www.ceia.net

UPCOMING EVENTS 2026

C-IED COE main activities 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.

WIT Revision WS
19-Jan

DOMEX Train the Trainer 26
TBD

Analyst Notebook User Course (ANUC) 26.1
6-Feb

C-IED Staff Officer Course 26.1
2-Mar

Annual Discipline Conference (combined 3 COE's)
24-Mar

Document & Media Exploitation Course (DOMEX) 26.1
11-May

NATO Weapons Intelligence Team Course (WIT) 26.1
11-May

Analyst Notebook User Course (ANUC) 26.2
28-Jun

Annual C-IED & TE Conference 2026
15-18 Jun

C-IED Staff Officer Course 26.2
22-Jun

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

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

C-IED Staff Officer Course 26.3
26-Oct

Analyst Notebook User Course (ANUC) 26.3
9-Nov

AtN Operational Course (ATNOC) 26.2
9-Nov

Steering Committee 2026
17-Nov

WIT TDC 26
30-Nov

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.

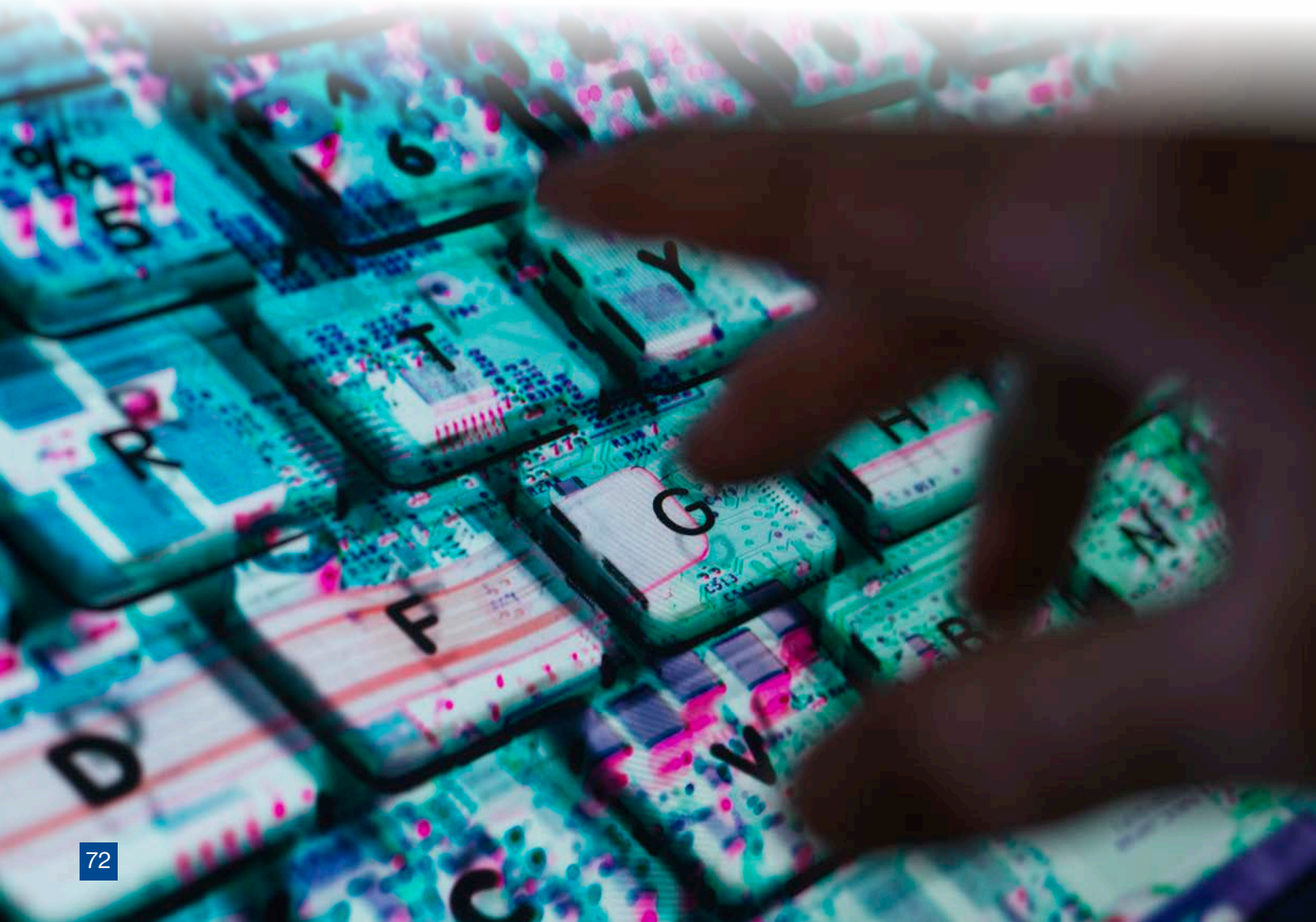
By consolidating expert analysis from all branches of the COE and transforming it into clear, accessible products, the Centre ensures that its expertise directly contributes to improved situational awareness and better-informed planning.

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

- Pro-DAESH LAMANHO publishes instructions for cellular-based radio control manufacture.
- Online proliferation of technical instructions for homemade primary explosives.
- Russian handbook for UAS chemical improvised munitions.
- Ukrainian FPV Explosive-laden drones against Russian Strategic Air Force.
- Pro-DAESH online technical instructions for homemade explosives.
- Pro-DAESH LAMANHO publishes online video on HME HMTD manufacture.

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.

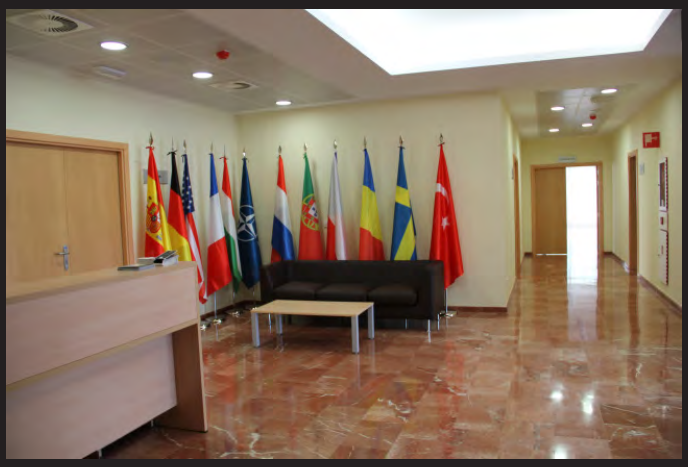
Your technology deserves to be seen. Your brand deserves to be trusted.

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