YOU ARE IN THE C-IED

CHESSBOARD

INSIGHTS FROM NATO's C-IED EXPERTS

JUN 2025 | ISSUE 03

Special Issue

Defeating the Hidden Threat: C-IED Lessons from Ukraine

C-IED COE

Annual Conference-25

COUNTERING IED IN SUPPORT OF MULTI-DOMAIN OPERATIONS

09 -12 June 2025 Málaga | Spain

NATO OTAN

Accredited COE

EDITORIAL STAFF

Director
COL Javier Corbacho Margallo (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
COL Umut Cetin (TUR A)
LTC José Manuel Rufas Simón (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)
MAJ Juan Manuel Mancilla López (ESP MC)
MAJ Peter van Achterberg (NLD A)
MSGT David Herráiz López (ESP 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,

It is my pleasure to welcome you to this special issue of our Chessboard, dedicated to exploring the multifaceted role of C-IED in the ongoing Ukraine-Russia conflict. From an evolving threat landscape to technological innovation, hybrid actors such as Wagner, and operational lessons learned, this edition reflects our collective effort to understand, adapt and improve our C-IED capabilities in modern warfare.

At the heart of this work remains the C-IED Centre of Excellence, whose mission endures: to serve as the main hub for the global C-IED community of interest. We continue to pursue this role with commitment, diligence and curiosity-supporting NATO's transformation, operational readiness, and the constant evolution of C-IED doctrine and training.

This issue also marks the beginning of a new chapter for Chessboard itself. For the first time, the magazine is published with the support of private sector sponsors, allowing us to deliver a professionally printed edition during our C-IED Annual Conference (CIEDAC). This partnership expands our reach and underlines the growing relevance of public-private collaboration in addressing the IED threat.

Looking ahead, CIEDAC 2025—to be held in Málaga this June—will bring together experts, military professionals, law enforcement, academia and industry in a consolidated event that replaces our former Technology Workshop and Interagency Workshop formats. It represents a streamlined, strategic platform for engagement across domains and sectors.

On a more personal note, this will be my final contribution as Director of the C-IED COE. As I am preparing to conclude my tour of duty in August, I would like to express my deepest gratitude to the exceptional staff of the Centre, and to all the members of the C-IED community who have shared this mission. Your dedication, professionalism and hard work have been a constant source of inspiration.

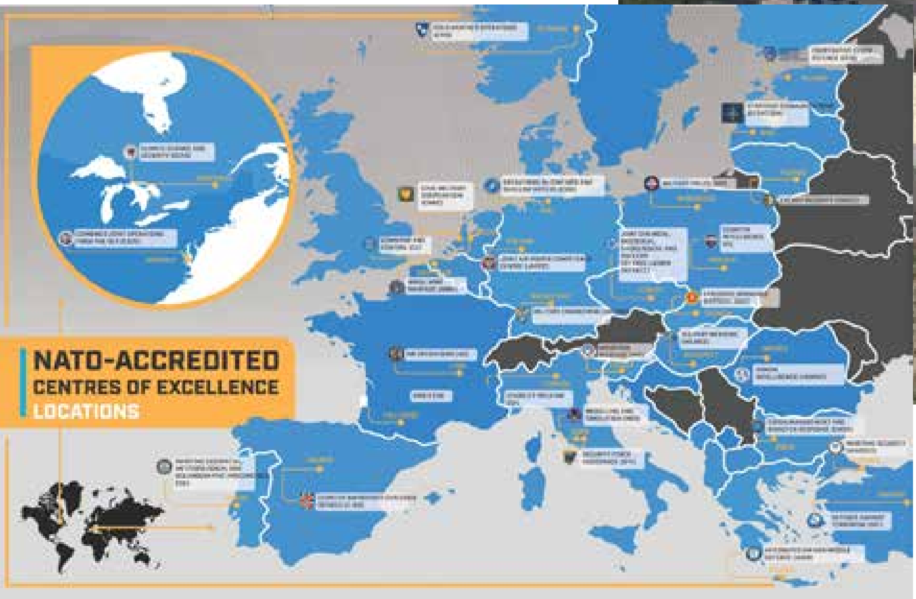
I also take great pride in introducing my successor, Colonel Javier Sanz (ESP Army), who will bring deep experience and vision to the role. I am confident he will guide the Centre with strength, clarity and purpose into its next chapter.

Thank you once again for your trust and partnership. Enjoy this issue, and I look forward to seeing many of you in Málaga.

With warm regards,

Colonel Javier Corbacho

Director, C-IED Centre of Excellence



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)

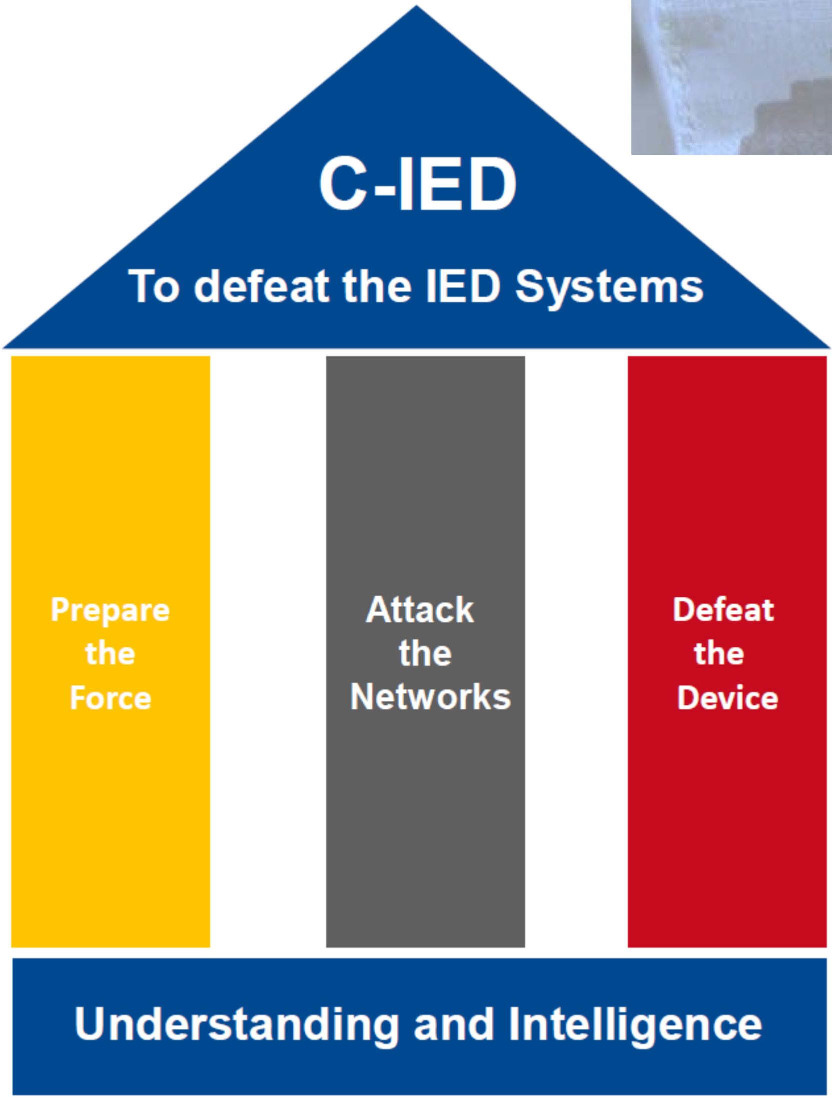
MORE INFO
act.nato.int/about/centres-of-excellence

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.

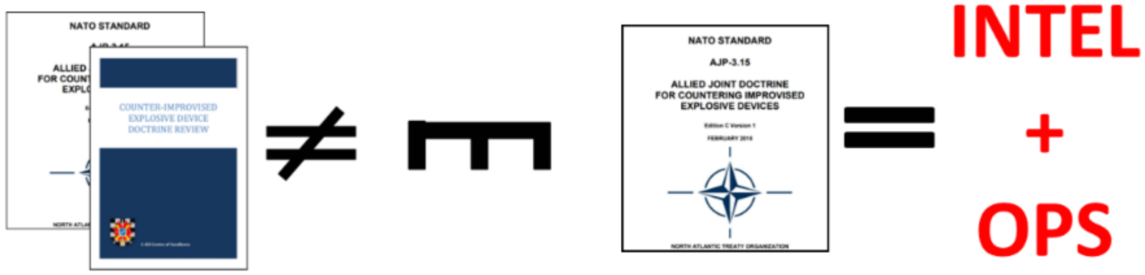
The C-IED COE is a proud member of the COE community

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 THE C-IED...

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


NATO STANDARD
COUNTER-IMPROVISED EXPLOSIVE DEVICE DOCTRINE REVIEW
≠
NATO STANDARD
AJP-3.15
ALLIED JOINT DOCTRINE FOR COUNTERING IMPROVISED EXPLOSIVE DEVICES
NORTH ATLANTIC TREATY ORGANIZATION
=
INTEL
+
OPS

C-IED COE HIGHLIGHTS

Quality Assurance: Raising the Bar in NATO Education and Training

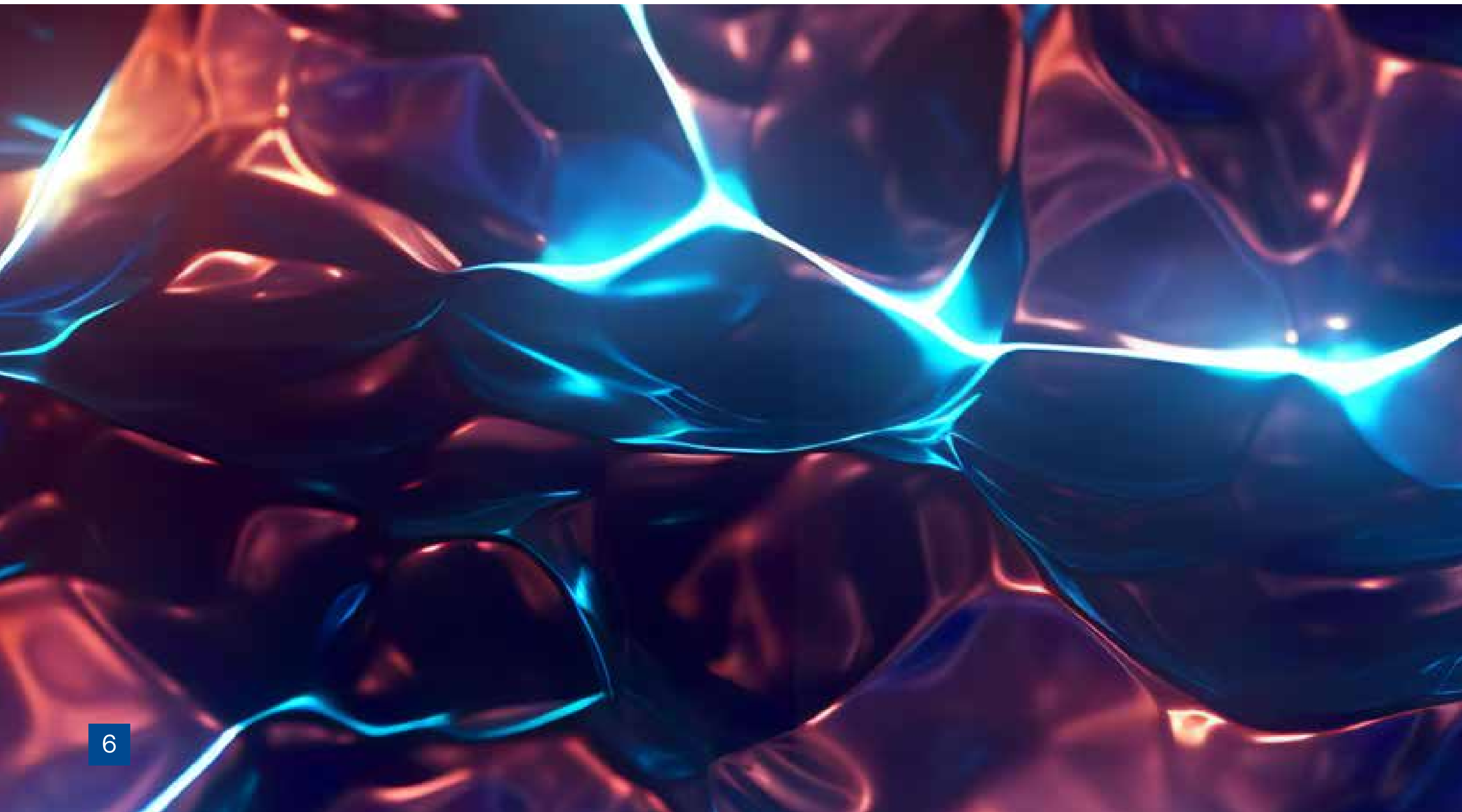
Our recently published 2024 Annual Quality Assurance Report paints a clear picture: the C-IED COE not only upheld its commitment to NATO education and training excellence but also laid solid groundwork for strategic transformation aligned with the Alliance's 2030 vision.

Following its unconditional NATO QA reaccreditation, effective from January 2025 through 2030, the Centre has reinforced its role as a key enabler in Multi-Domain C-IED education, doctrine development and innovation. The report highlights strong course execution, continued instructor development, digital transformation and growing resilience—all backed by a rigorous Quality Management System.

Education & Training: Delivering Results Across the Board

With 240 students trained across 8 course types from the C-IED Staff Officers Course (CSOC) to the advanced DOMEX programmes—the Centre achieved a **91.94% graduation rate** for NATO-approved offerings. Notably, the **WIT TDC and Advanced DOMEX** courses have moved from pilot status to formally listed in the NATO Education & Training Opportunities Catalogue (ETOC), reflecting growing demand for advanced technical skills in modern conflict scenarios.

The Centre also continued to adapt and improve. **Last-minute cancellations** and **fluctuating attend-**



ance were recognized as areas needing tighter management—prompting policy changes and timeline adjustments for 2025.

Quality Management: A Culture of Continuous Improvement

Internally, the Centre maintained a robust QA system, focusing on course evaluations, instructor feedback, and post-course impact surveys. Digital feedback collection via QR-code-based forms became standard across all offerings, and post-course follow-ups saw participation improve from 17% in 2023 to 27.5% in 2024—a promising step in closing the feedback loop.

The launch of a Staff Satisfaction Survey revealed strong institutional expertise while also identifying inter-branch communication as an area for growth. This will guide internal development efforts in the years ahead.

Multi-Domain Operations and Digital Transformation: Not Just Buzzwords

2024 marked a decisive shift toward integrating Multi-Domain Operations (MDO) into education and doctrine. Courses like ATNOC and WIT already include MDO-relevant modules, and staff started completing ADL 374 on MDO, which becomes mandatory for all students in 2025.

On the digital front, the Centre advanced its use of SharePoint, designed new AI and 3D modelling-based learning scenarios, and established the foundation for an alumni network to strengthen its Community of Interest (CoI).

Looking Ahead: Challenges and Opportunities

Among the priorities for 2025:
Launching ADL prerequisites for all listed courses.
Developing a certified internal instructor pool for the ANUC course.
Implementing an updated and improved newcomer induction programme.
Enhancing knowledge management with improved SOPs and archiving procedures.

These initiatives not only aim to future-proof the Centre but also reflect its commitment to institutional resilience, operational relevance and strategic alignment with NATO transformation goals.

Conclusion

The 2024 QA Report confirms that the C-IED COE remains a cornerstone of NATO's C-IED education and innovation ecosystem. By continuing to evolve and adapt—while maintaining quality at its core—the Centre is poised to meet the complex demands of future operating environments.

C-IED COE Lodge Supports Ukrainian Students During Humanitarian Demining Training

From 6 September 2024 to 20 January 2025, the C-IED COE supported a total of 101 Ukrainian soldiers participating in two rotations of the International Humanitarian Demining Course. The training was conducted by the Spanish Army's International Demining Centre, located within the Engineers Academy compound in Hoyo de Manzanares.

The first course hosted 51 students from 6 September to 9 November, followed by a second rotation of 50 students from 9 November to 20 January. In both iterations, the C-IED COE Lodge provided accommodation for them, offering not only logistical support but also a comfortable and supportive environment that contributed directly to the success of the training.

Student feedback was overwhelmingly positive, highlighting the quality of the facilities, the welcoming atmosphere, and the strong camaraderie that developed among participants. This positive environment played a key role in reinforcing learning outcomes and morale throughout the duration of the programme.

By providing this support, the C-IED COE reaffirms its commitment to multinational cooperation, operational readiness and the humanitarian imperative of mine action. It also illustrates how NATO structures can play a meaningful role in capacity building efforts for partner nations affected by conflict.

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

NATO OTAN

Accredited COE

C-IED COE

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

MORE AT: nato.int

HOW COEs
to request support
TRANSNET
Register NOW!
required@nato/mod/gov/mil...
JOIN NOW
COE COMMUNITY
with
RFS TOOL
SKILLS
EXPERIENCE
FREE
SUBMIT REQUEST
Communicate PROCESS
Feasible
Assessment
Approved
Completed
ENJOY!

ENGAGE!

EVENTS

Combined Annual Discipline Conference

The first Combined Annual Discipline Conference (CADC) took place from 4 to 6 March at the C-IED Centre of Excellence (COE) in Hoyo de Manzanares, Spain. Hosting this event with three different but well-connected disciplines made these days special. The connection between all three (Military Engineering, Energy Security and C-IED) is their common Requirement Authority (RA). That is why this conference was just the appropriate solution.

Integration of all domains is key to stay a relevant source of knowledge and practical resource for NATO's transformation and Multi-Domain operations. That is why, during this Conference, experts from NATO Command and Force structure as well as from other COEs, exchanged ideas about the current and upcoming requirements.

With this outcome, the Discipline Head started working with the Requirement Authority in SHAPE to develop solutions for the gaps/requirements detected. The final product of this conference was the agreed Discipline Alignment Plan, which gives a more detailed way ahead for next year.

By addressing the needs and gaps across all three disciplines together, the CADC provided an efficient platform for collaboration, ensuring a more integrated approach to NATO's capability enhancement efforts.

Fostering Integration and Innovation: Highlights from the First NATO Combined Annual Discipline Conference at the C-IED COE

Maintaining relevance as a **knowledge hub** and **practical resource** for **NATO's transformation** and **multi-domain operations** demands close coordination across domains. The CADC leveraged contributions from experts across the NATO Command and Force Structures, other Centres of Excellence, and key stakeholders. Discussions centered on identifying both current and future requirements, critical to operational success.

The outcomes of these exchanges between experts will guide the **Discipline Heads**, as they work closely with the **Requirement Authority** at **SHAPE** to address capability gaps and define actionable development pathways. One of the major deliverables from the conference is the jointly developed **Discipline Alignment Plan (DAP) 2025,** which provides a clear roadmap for next year's collaborative efforts.

Purpose and Focus Areas

Throughout the three-day event:

- Each discipline conducted its own Annual Discipline Conference (ADC) to review its 2024 Discipline Alignment Plan (DAP), update Education and Training (E&T) opportunities, and coordinate efforts to streamline resources and synchronize activities.

- Discussions included identifying training requirements, potential new courses and seminars, and priorities for conducting **Training Needs Analyses (TNA)** during 2025.
- A dedicated forum allowed Communities of Interest to express and align individual and collective training requirements, contributing to NATO's training integration cycles (e.g., e-ITEP, ETOC, ePrime).

Strengthening the Community of Interest

Through this conference, the C-IED COE reaffirmed its commitment to fostering synergy across disciplines, enhancing operational effectiveness, and supporting NATO's continuous transformation to meet evolving security challenges.

The CADC not only strengthened the coordination between disciplines but also highlighted the vital role that integrated education and training efforts will play in preparing NATO forces for the complexities of the modern security environment.

The C-IED COE looks forward to continuing its work alongside its Military Engineering and Energy Security counterparts, helping ensure that NATO remains agile, innovative and fully capable of responding to current and future threats.

C-IED Annual Discipline Conference 2025
C-IED
COE
1st Combined ADC
4-6MAR 2025, C-IED COE
Hoyo de Manzanares, Madrid-Spain

Threat Dynamics in the Ukrainian Theatre of Operations

After talking with our C-IED related Ukrainian colleagues, the most evident consequence from the current conflict is not only based on the loss of lives and territory, but also on the extremely high degree of contamination of terrain by Unexploded Ordnance (UXO), including Improvised Explosive Devices (IEDs), a fact that is expected to persist long after the end of the armed conflict.

Unfortunately, the analysts at the C-IED Centre of Excellence were not wrong when they anticipated a potential massive use of IEDs (including explosive-laden drones) in Ukraine, along with the implication of non-state actors (although in most cases they could be state-sponsored) in the conflict.

Nonetheless, the use of IEDs after the Russian invasion in late February 2022 is just a continuation of the trends started in 2014 with the crisis in the Donbas.
In Ukraine, not only the numbers are higher than expected for such a "conventional warfare", but the quick evolution and huge variety of different types of IEDs, associated Tactics, Techniques & Procedures (TTPs), components, technologies... are beyond belief.

At the beginning of the current conflict between Ukraine and Russia in 2022, the use of IEDs was mainly focused on victim-operated "booby-traps", using military conventional munitions emplaced in an improvised manner, and on the manipulation of conventional munitions.

Little by little, a smart imitation of TTPs from other areas of operations (e.g. Iraq, Syria...) was developed by the Ukrainian side in their legitimate aim of defending against the invasion. This involved dropping improvised munitions from commercial-off-the-shelf (COTS) Unmanned Aerial Systems (UAS) and using simple IEDs in sabotages and ambushes.

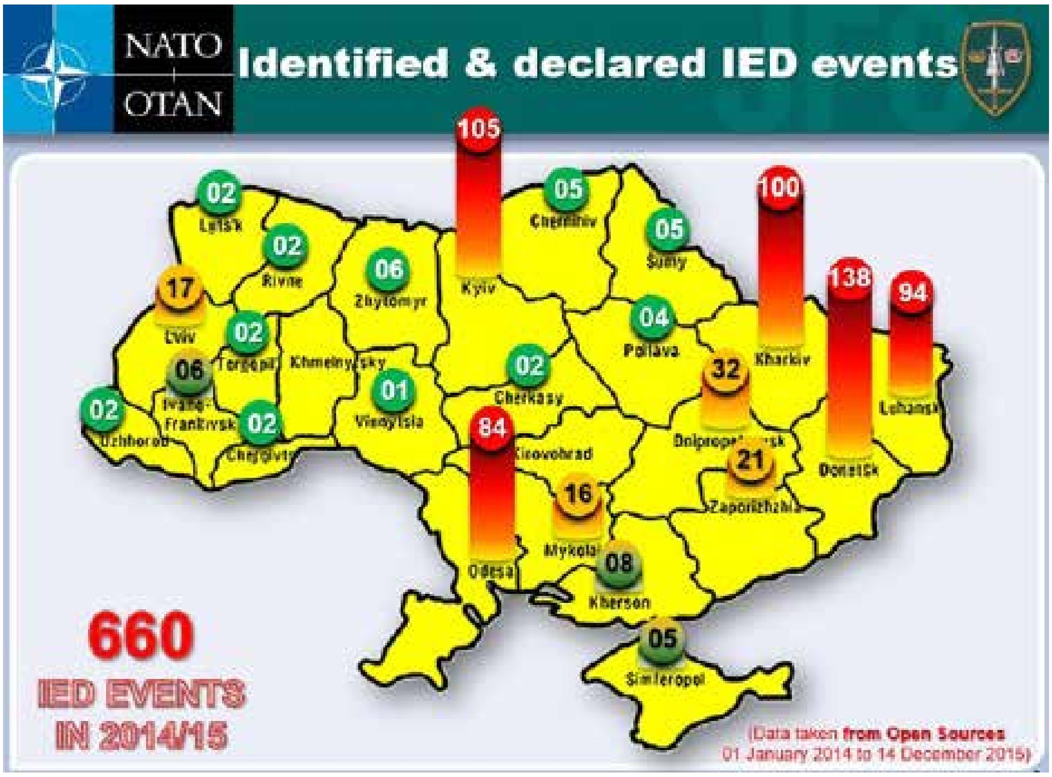


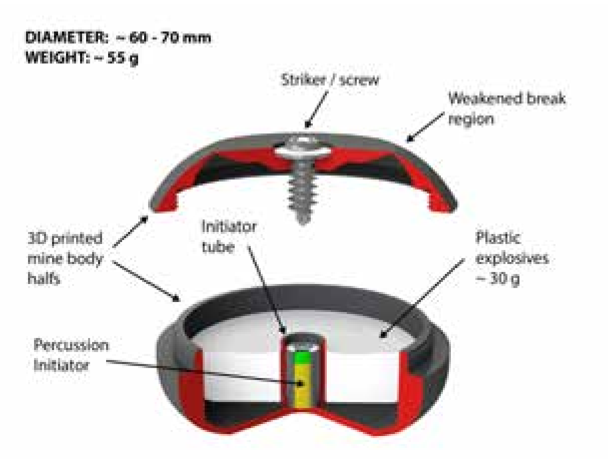
Figure 1 – Metrics about the events with IEDs in Ukraine 2014-2015 (Source – NATO Joint Force Command Brunssum Headquarters)

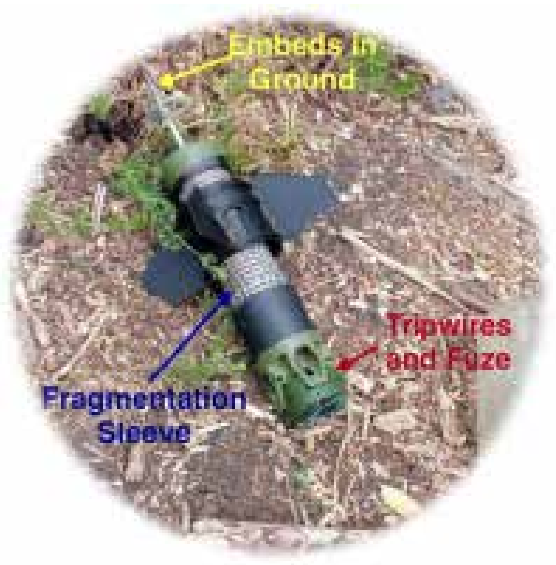
The next step consisted in modifying conventional munitions with additive manufacturing (3D-printing) for UAS (e.g. tails, fuzes…) and using anti-lifting devices inside the landmines or their respective fuzes.
Regarding the development of new ideas about IEDs designs and/or the development of new TTPs in the use of IED, the Ukrainians have been taking the initiative, but the Russians are being agile in copying (even improving) and adapting those advances in their own IEDs.

The current use of IEDs evidences the relevance of technologies in the field of IED development: we can identify the design/manufacture of improvised munitions with 3D-printing technologies (e.g. copies of scatterable munitions and landmines) and the development of advanced victim-operated electronic devices (e.g. anti-handling, magnetic influence, self-destruction, time delay… or even a combination of some of them inside the same device).

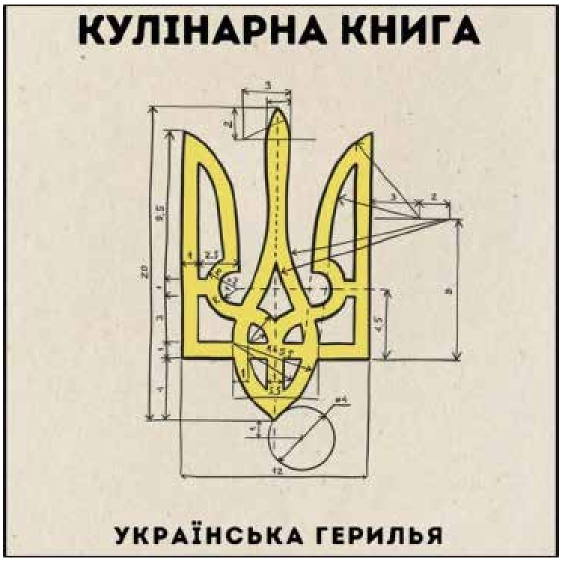
As a conclusion, the most worrying outcome from the wide use of Improvised Explosive Devices and associated Tactics, Techniques and Procedures is the uncontrolled and multi-sourced distribution of manuals, instructional videos, tutorials and ideas about how to manufacture and use IEDs, which both Ukrainian and Russian actors are making available through the Internet.

In fact, most of the violent extremist organizations are redistributing training material from Ukrainian area of operations in their own online sites and the IEDs TTPs from Ukraine have migrated to other areas of operations.

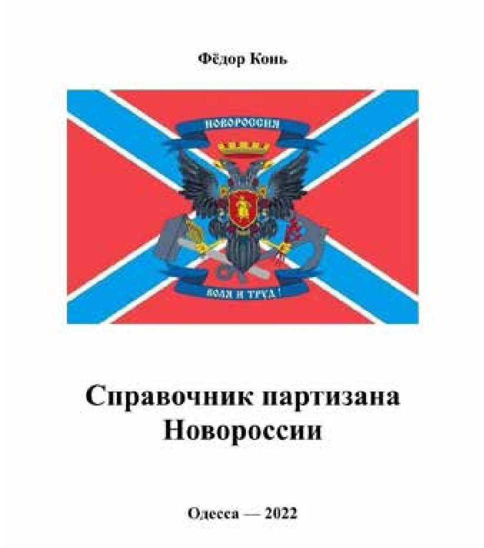




Figures 2 and 3 – 3D-printed scatterable improvised munitions used in Ukraine (Source – www.armourers-bench.com, X, TELEGRAM)


КУЛІНАРНА КНИГА

УКРАЇНСЬКА ГЕРИЛЬЯ


Фёдор Конь

Справочник партизана
Новороссии

Одесса — 2022

Figure 4 – Covers of Ukrainian & Russian IEDs manufacture handbooks available online (Source – SCRIBD, TELEGRAM, VK)

C-IED related observations from Ukrainian Theatre of Operations

There are three main facts which are strongly conditioning the potential application of the Countering Improvised Explosive Devices (C-IED) approach in the Ukrainian theatre of operations:

1. The origin of the current conflict was not on February 2022 (Russian invasion of Ukrainian territory), but it can be traced back to the uncontrolled multinational (two-block) hybrid evolution of the Ukrainian "civil war" between the pro-Russian separatist forces from Donbas region (Donetsk and Luhansk) and the rest of the Ukrainian territory.

2. Contrary to several Western perspectives, the Russian-Ukrainian conflict is not a pure (and strongly wished) return to a conventional approach of a state actors' warfare, but a mixture of Multi-Domain operations in a hybrid threat environment which includes:

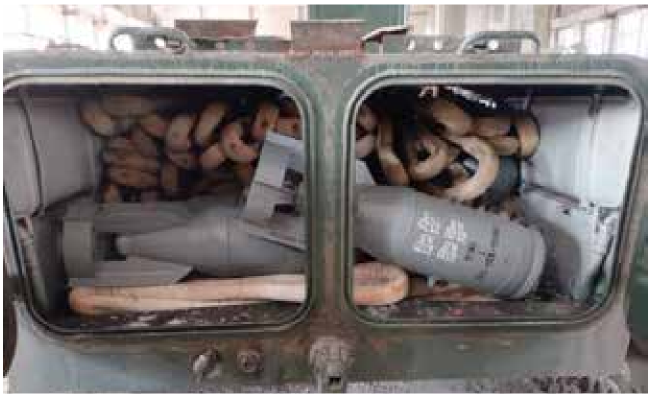
- Conventional forces taking benefit of unconventional Tactics, Techniques and Procedures (TTPs) in combination with the application of conventional warfare.

- Unconventional forces making use of conventional and unconventional TTPs.

3. There is a huge relevance and utilization of the online environment in all the aspects of the conflict.

Accordingly, and against the expected return to the military employment of conventional armament and TTPs, the use of IEDs has been dramatically growing with the progression of the crisis in Ukraine. This would, in principle, make the C-IED approach still valid and applicable.
We have witnessed how the IEDs have been used not only in the land domain, but also in the maritime/water (e.g. unmanned surface vehicles and improvised sea mines) and air domains (e.g. explosive-laden drones), while taking a smart benefit from the online exploitation of their success after attacks with IEDs and the proliferation of technical instructions for the manufacture of IEDs distributed through social media (so the cyber domain is also included).

With regards to the Attack the Networks approach, the Ukrainian authorities were effectively mapping the adversary human networks outside the Donbas region and dismantling their capabilities to carry out attacks using IEDs. This was possible thanks to an extensive application of human intelligence over pro-Russian groups all around the country and the pre-identification of their irregular activities.



Figures 1 and 2 –Samples of the use of an armoured vehicle borne IED and an underbelly attached IED to civilian car in Ukraine (Source – X)

The application of Technical Exploitation (TE) in the benefit of technical intelligence is considered brilliant (especially from the Ukrainian side) and, although the outputs from TE have not been effectively applied from an Attack the Networks perspective to undermine the capabilities of adversary human networks, the TE outcomes seem to have been quite useful for tactical analysis.

From NATO's point of view and under their standards, both the Ukrainian and Russian developments of the Defeat the Device pillar are still under the minimum requirements for the Allied skills, as far as the detection, neutralization and mitigation of explosive ordnances and Military Engineering (MILENG) are concerned. Nonetheless, these developments have been tactically effective and have provided real battle experience to the first responders.

Regardless of the external support in education and training, especially regarding C-IED, the development of the Prepare the Force pillar by the Ukrainian forces could be considered realistic, adaptive and effective, although it is still different than in NATO countries.

Maybe all the previously considered observations could be a bit surprising if we take into consideration that the Ukrainian Armed Forces adopted as their official C-IED doctrine a direct translation into Ukrainian language of the AJP-3.15(C) "Allied Joint Publication on Countering Improvised Explosive Devices (C-IED)".

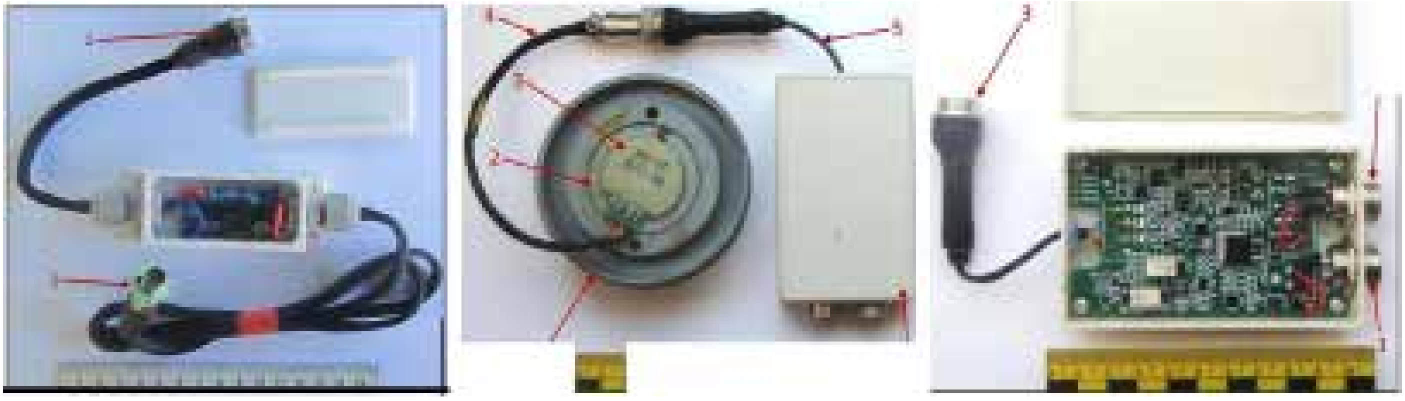
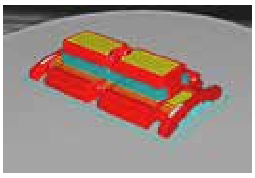


Figure 3 – Images from a Ukrainian handbook on TE of explosive-laden drones (Source – Telegram)

Additive Manufacturing in the Ukraine-Russia Conflict: Operational Innovation and Asymmetric Threats

The ongoing conflict in Ukraine has become a testbed for emerging military technologies, with Additive Manufacturing (AM), commonly known as 3D printing, playing a surprisingly prominent role. Originally developed for prototyping and civil applications, AM has been rapidly integrated into tactical operations, enabling both state and irregular forces to innovate under pressure, circumvent supply constraints, and enhance operational flexibility on the battlefield.

Tactical Utility and Battlefield Applications



3D printing allows the in-field production of a wide range of military assets. In the Ukraine-Russia conflict, both sides have used it to manufacture drone bomb release systems, munition housings, grenade components, Improvised Explosive Devices (IEDs), and mission-specific medical tools, such as tourniquets and splints. These tools are not rudimentary—many demonstrate iterative improvement, battlefield testing and adaptation for mass replication using commercial—grade equipment.

For instance, Ukrainian engineers developed light-sensor-triggered mechanisms that allow commercial drones to deploy munitions with precision, using nothing more than 3D-printed clamps, servos and simple electronics. These devices evolved into modular release units with Arduino control systems, offering combat effectiveness at a fraction of the cost of traditional loitering munitions.

The "Ukrainian Archive": Open-Source Weaponization

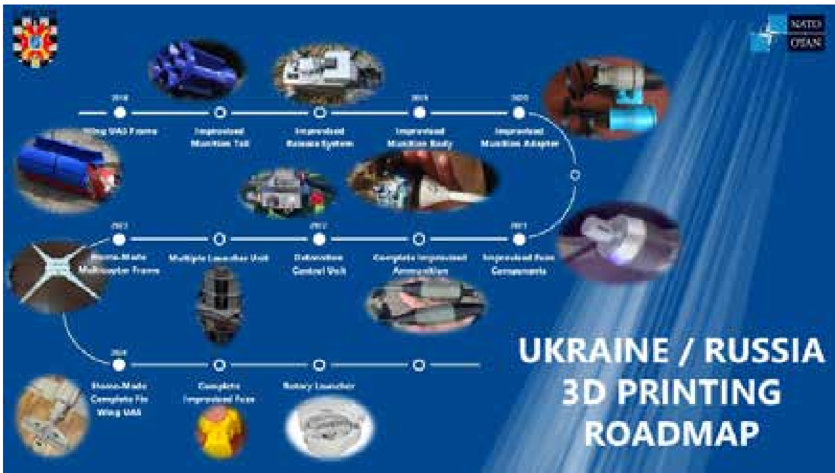
In May 2024, pro-Russian hackers leaked a file archive nicknamed the "хохлоархив" ("Ukrainian Archive"), which was shared widely via Telegram. The archive contained hundreds of 3D-printable files developed by Ukrainian volunteers and combat engineers. Among them were:

- Aerial-dropped improvised explosive munitions.
- 3D-printed drone payload release mechanisms.
- Fuze housings and grenade bodies.
- Training aids (e.g. inert mines and EOD replicas).
- Starlink terminal accessories (antenna mounts, signal boosters).
- Medical devices, such as splints and braces.

These designs were accompanied by printer settings, materials lists and even instructional videos-removing many of the barriers previously associated with field manufacturing. The archive's release highlights the potential for unregulated proliferation of battlefield technology.

Strategic Risks and Threat Diffusion

The democratization of weaponized AM creates urgent challenges. Files of this nature are now accessible on open-source platforms and encrypted channels. Violent Extremist Organizations (VEOs) could leverage this content to locally manufacture functional IED components or drone enhancements without requiring centralized infrastructure.



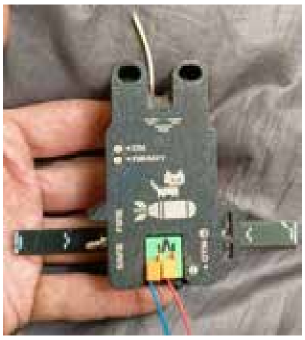
This threat is magnified by the fact that many of the materials and printers used are indistinguishable from those used by civilians or hobbyists. Furthermore, tutorials and community support have drastically lowered the technical threshold for producing dangerous equipment.

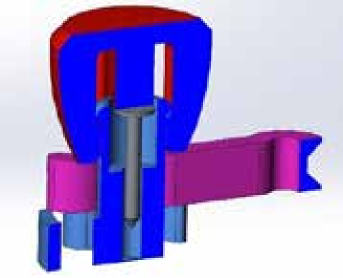
Defense and Counter-Proliferation Implications

Defense communities must take the lessons of Ukraine seriously:

- **Integrate AM into logistics**: Deployable fabrication units should be standard in modern expeditionary forces.
- **Expand regulatory frameworks**: Track, classify and potentially restrict digital files with dual-use applications.
- **Monitor digital ecosystems**: Engage in counter-influence and intelligence operations to trace AM-related file-sharing among threat actors.
- **Train in AM-based operations**: Educate personnel on both the operational uses and countermeasures related to 3D-printed systems.

As AM continues to evolve, the line between traditional defense supply chains and home-made battlefield engineering will blur. The next phase of irregular warfare may be shaped less by access to weapons than by access to printers and blueprints.





References

20240724_S256_SENSITIVE_U-FOUO_C-IED_CoE_Report_Threats_posed_by_the_use_of_3D_printing_technologies_in_UKR-RUS_conflict.

Observations derived from open-source intelligence monitoring, May–July 2024.

Telegram posts shared by "RVvoenkor" and similar pro-Russian channels.

Files from the leaked "хохлоархив" archive, reviewed in June 2024.

Repositories and forums: Thingiverse, Cults3D, GitHub, DefCAD.

Interviews with Ukrainian drone technicians and volunteer engineers, April 2024.

Field reporting and analysis provided by NATO C-IED COE team.

Improvised Passive Protection/Mitigation Measures against Explosive-laden Drones

1. AIM:

The purpose of this article is to explain the pros and cons of improvised passive protection/mitigation measures (cope cages/anti-drone nets/decoys/dummies) against the effects of explosive-laden drone attacks.

2. INTRODUCTION:

One of the fastest-growing industries in the world is the consumer drone market, making drone technology practically accessible to everyone. The number of drone-related incidents in the vicinity of airports, public events and military installations has drawn the attention and concern of the civil authorities in charge of public safety and law enforcement because of their growing prevalence.

Since the beginning of its activities in Syria, DAESH has made use of drones as means of collecting imagery intelligence. By late 2016, DAESH had begun weaponizing drones to attack Peshmerga forces in Northern Iraq; armed drones were subsequently used against Iraqi army targets during the campaign in Mosul, and later in the battles that took place over Eastern Syria during the second half of 2017.

On the other hand, the 2nd Nagorno-Karabakh war, the war in Ukraine, as well as other conflicts around the world, have shown the significant results that can be achieved with drones and have led to a shift in defence industry spending.

During the initial Donbas war from 2014 to 2017 and since February 2022, when the Russian invasion of Ukraine started, both sides have been using explosive-laden drones to attack various type of targets.

Drones have added a revolutionary component to the war, allowing for more precise strikes. As a result of this success, rivals had to take some measures against the wide range effects of this easy, cheap and effective weapon of choice, not only in the Russian war against Ukraine, but also in other conflict zones.

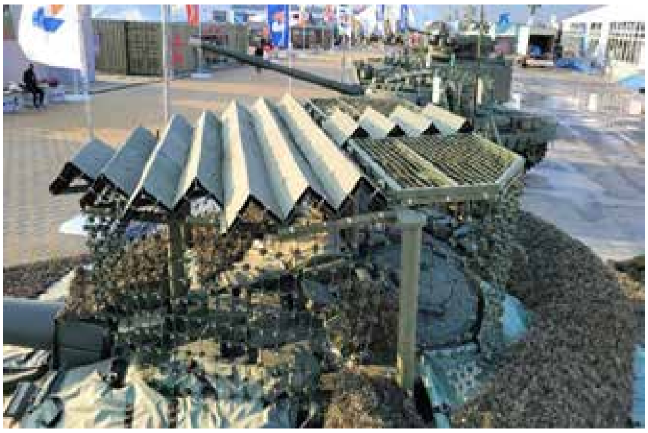
3. THE MEASURES TAKEN BY RUSSIA AND UKRAINE:

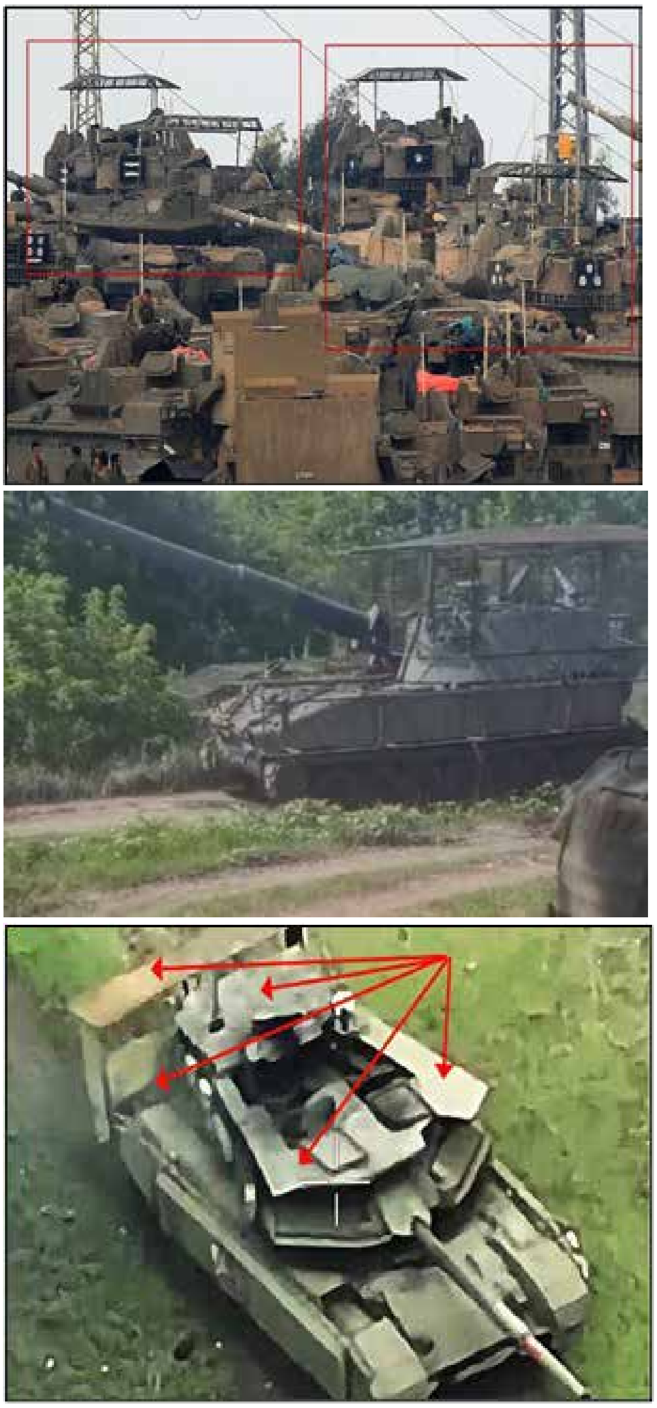
Since the beginning of the war, both sides took some passive protective measures against explosive-laden drone attacks and published the handbooks/manuals on best practices, material and procedures for protecting military facilities, ground defensive positions, military vehicles, main battle tanks, military aircrafts, submarines and even for civilian installations.

To properly explain the measures taken, we may start with the general description of what a "Cage Armour" is and how it works. A "cage" or "slat armour" is a type of passive protection/mitigation measure, in general consisting of high-strength metals, with a grid-like texture around the desired area, to mitigate the effects of all kinds of conventional or improvised munitions, especially anti-tank munitions, including drones and drone-delivered munitions. It works as a physical barrier, disrupting the trajectory or detonation mechanism of incoming projectiles and it helps to mitigate the impact of a drone collision, a blast and the fragmentation effects of explosive devices dropped from a drone.

By introducing a stand-off between the barrier and the target, these munitions greatly lose their effectiveness, and this grants the personnel some level of protection.

You may see some samples of cope cage usage in Figures 1-3. Additionally, Russian usage of two symmetrically arranged armour plates flanking the tank turret instead of cope cages (Figure 4) was displayed





Figures 1-4

as a new protective measure/structure.

These protective measures/structures are customized by countries, based on the threat level in their area of responsibility, as a lesson learned topic from recent conflict areas, to enhance their capabilities for mitigating the effects of all kinds of conventional or improvised munitions, especially anti-tank munitions, including drones and drone-delivered munitions.

There are also some protective measures/structures (drone nets) on the military facilities (trenches, bunkers, etc.) against explosive-laden drone attacks in Figure 5.

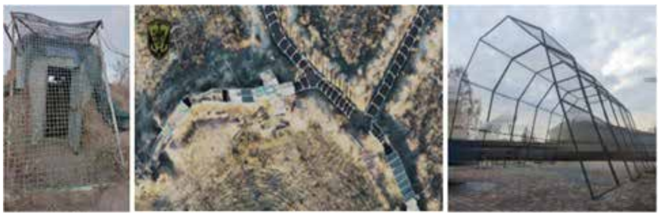
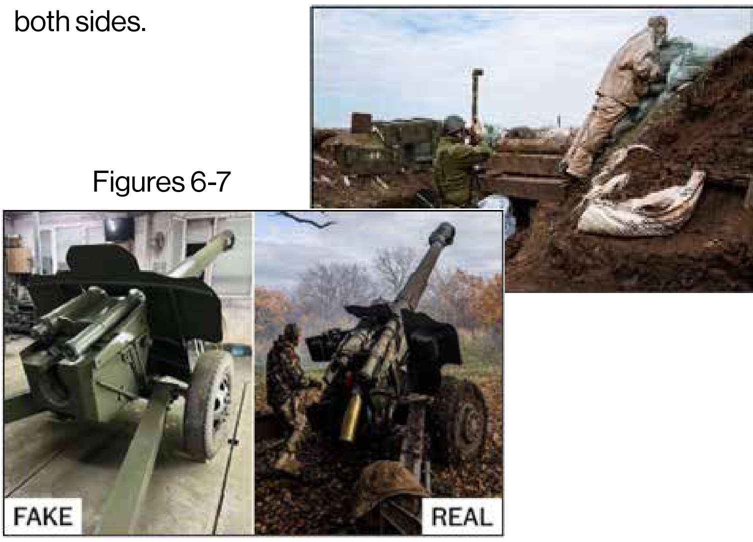


Figure 5

Moreover, Russia and Ukraine have been using decoys/dummies of armoured vehicles and military systems (Figures 6-7) to deceive enemy drones, forcing their adversaries to waste resources while protecting their real vehicles/systems. Therefore, the constant waste of valuable munitions and drones in traps has led to increased frustration and demoralization on both sides.



Figures 6-7

4. ADDITIONAL MEASURES TAKEN BY RUSSIA:

In August 2023, Russia came under attack, in the biggest drone assault on its territory since it launched its invasion of Ukraine. In the city of Pskov, near the Estonian border, several transport planes were reportedly damaged when drones targeted an airport.

Earlier in August, Ukraine had carried out drone strikes on bases that house supersonic bombers deep in Russian territory – in what appeared to be an effort to make a dent in Russia's air power, which has been a major obstacle for Ukraine's counteroffensive (Figure 8).

Figure 8

Ukraine claimed to have destroyed four aircraft, while Russian sources said the aircraft had been "damaged"

As a counter manoeuvre/action, Russia has covered aircrafts with car tires, thus protecting them from Ukrainian drones. These tires are positioned along the entire length of both wings, especially on the internal/external fuel depots and a small segment of the upper fuselage. Satellite imagery shows how Russia has acted against Ukrainian drone attacks (Figure 9).

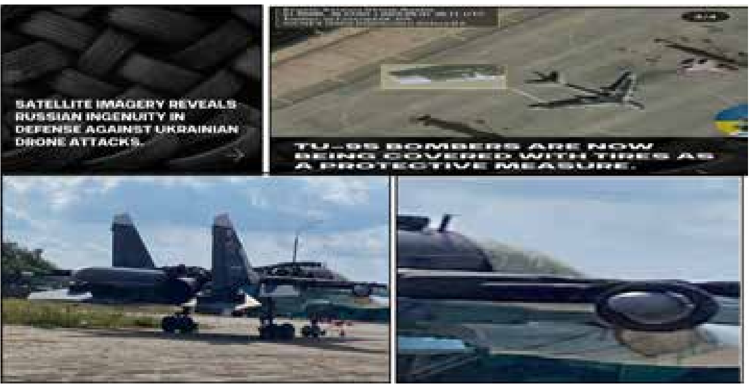

SATELLITE IMAGERY REVEALS RUSSIAN INGENUITY IN DEFENSE AGAINST UKRAINIAN DRONE ATTACKS.
TU-95 BOMBERS ARE NOW BEING COVERED WITH TIRES AS A PROTECTIVE MEASURE.

Figure 9

Although this approach is not an approved way of protection/mitigation, it has been an improvised countermeasure. The underlying rationale for this kind of usage is most likely the belief that these tires may mitigate the impact of a drone collision, or of the blast and fragmentation effects of the explosive devices dropped from a drone. They may also protect planes from collateral explosions and reduce the thermal/IR image of the planes in order to complicate the guidance of a drone during the last part of the attack.

In addition to this measure, new posts/photos showing the installation of metallic nets designed to protect against drones have been published by some open-source accounts (Figure 10).

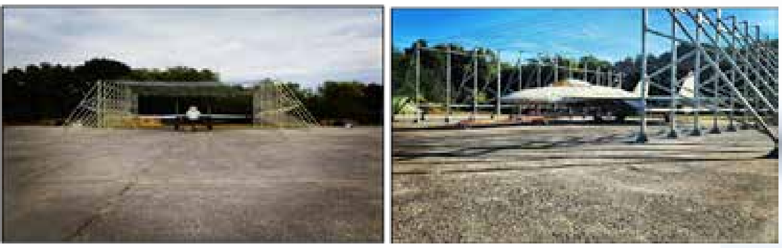


Figure 10

The logic behind this idea is most likely to make the drone collide with the net, or to cause the entanglement of the drone or the explosive devices dropped from a drone with the net. Thus, it would prevent the drone/IED from continuing its trajectory or it would allow an effective manoeuvre to mitigate the fragmentation effect. Additionally, the net may act as a visual obstruction for the drone's sensors and cameras, making it difficult for the drone operator to accurately navigate or target the vehicle.

Meanwhile, what is possibly the first sample of this kind in any navy's history has been reported. A "metal-framed structure (grills)" has been installed on a submarine's conning tower as a passive protection/mitigation measure for submarines, in line with the kind of add-on counter-drone top armour used by Russian forces in their tanks (Figure 11).

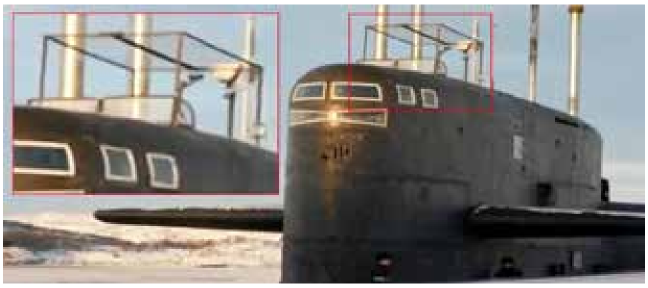


Figure 11

The mentioned submarine has been identified as the Tula, nuclear-powered submarine, serving within the Northern Fleet of the Russian Federation. The images below show the Russian submarine docked at Gadzhievo port in the remote Russian far Northern region of Murmansk (Figure 12).

The grill is thought to serve as a protection layer on top of the location where officers survey their surroundings using visual and electro-optical methods when the submarine emerges.

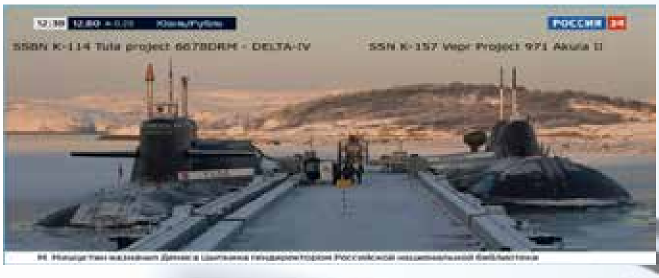

SSBN K-114 Tula project 667BDRM - DELTA-IV
SSN K-157 Vepr Project 971 Akula II
РОССИЯ 24

Figure 12

The possible rationale for this caged, metal-framed structure (grills), is to introduce a standoff between the command hatch / haul and to provide additional protection to those inside the command centre and their communication equipment.

Additionally, in recent days, it was published in open sources that some protection measures have also been taken to reinforce oil refineries against potential threats. "Cage systems (anti-drone net)", commonly referred to as "cope cages" have been installed (Figure 13).

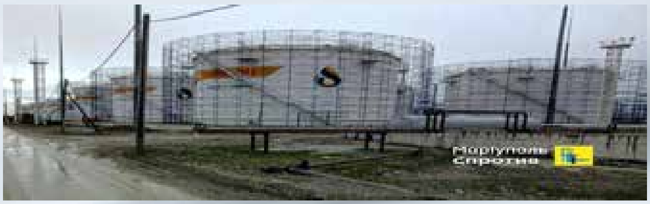


Figure 13

These commercially available cage systems could be described as the robust meshed metal structures that surround refinery buildings from all angles, anchored by mooring lines attached to metal stakes in the ground (Figure 14).

Figure 14

The decision to strengthen the refinery's defences may have been taken because of Ukraine's intensification of its attacks on Russian oil facilities since the beginning of the year, in order to reduce Russia's energy revenues and put additional pressure on its military spending budget.

4. CONCLUSION:

The use of all these passive protection/mitigation measures against possible threats can be considered improvised and low-cost solutions to the ever-evolving threat.

Although such applications can be innovative, they are far from having a confirmed level of protection/mitigation at both tactical and operational levels and are unlikely to deter advanced drone attacks. However, they certainly represent a progress in terms of increasing protection/mitigation levels.

Moreover, it should be noted that cage armours and the other passive protection measures are not complete solutions by themselves. The protection level of the materials, the number of layers and the distance from the target are critical issues that need to be evaluated in real time trials against advanced anti-tank weapons and other improvised munitions. Additional active defence systems and electronic warfare systems are considered more effective than this kind of passive protection measures.

In addition to these examples of improvised protection measures, the use of camouflage nets and decoys is also a passive protection measure, from both C-IED and Military Engineering perspectives.

In the ongoing Ukrainian conflict, and in the course of any conventional or hybrid war, opposing forces will constantly look for ways to attack, counterattack or repel each other. This constant battle of wits drives each force to develop innovative actions, while keeping them practical, rational and cost-effective.

References

Archambault, E. and Veilleux-Lepage, Y. (2020). 'Drone imagery in Islamic State propaganda: flying like a state', International Affairs 96.
www.bulgarianmilitary.com
www.defence-blog.com
www.twz.com
www.vk.com/milinfolive
www.en.defence-ua.com
www.telegraph.co.uk/world-news/2024/03/29/
https://x.com/mrfrantarelli/status/1770115036884697560?s=46
www.eurasiantimes.com
Different Telegram groups

Russian Private Military or Security Companies (PMSCs) in Ukraine?

Generics

First, we need to distinguish between the legal definition of a PMSC from NATO's perspective and the point of view of this NATO accredited C-IED COE.

According to Montreaux Document, "PMSCs" are private business entities that provide military and/or security services, irrespective of how they describe themselves. Military and security services include armed guarding and protection of persons and objects, such as convoys, buildings and other places; maintenance and operation of weapons systems; prisoner detention; and advice to or training of local forces and security personnel.

Moreover, in countering explosives devices, a PMSC is a network (NATO agreed term) that interconnects human and/or material nodes that may be identified, isolated or engaged.

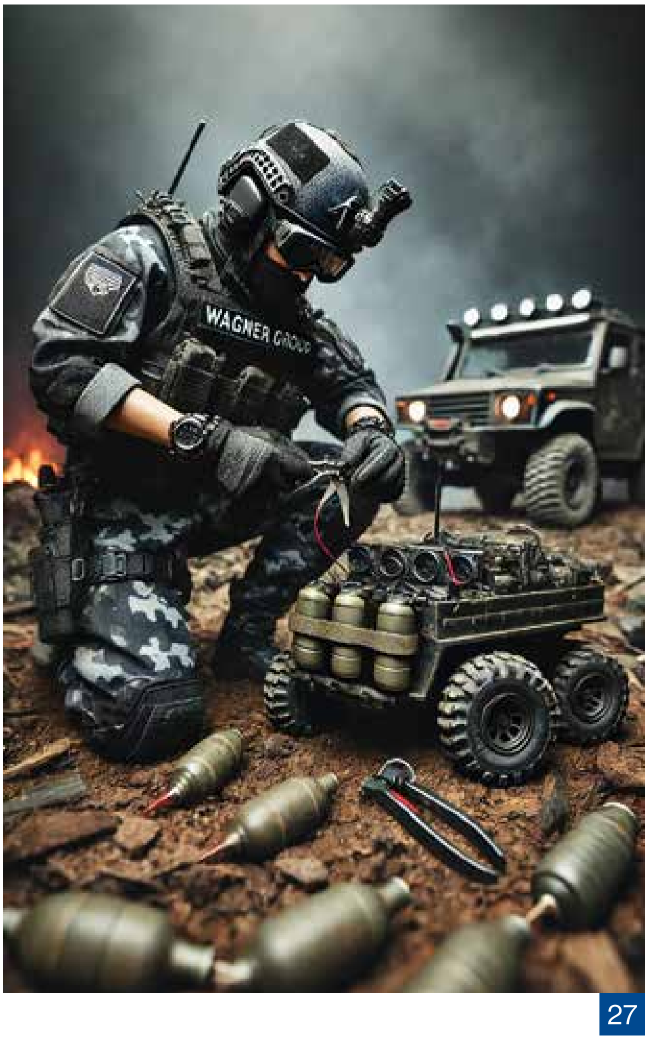
Summing up, we could say that a PMSC is a human threat network composed of trained personnel with enough equipment to use explosives in different scenarios and in multiple ways. Once again, Attack the Networks (AtN) is the main pillar to fight against the IED system, in this case focused on Violent Extremist Organizations (VEO), but not in terrorist groups, although nowadays there is an incredible transfer of knowledge using the cyberspace.

To clarify the process, first we have the "understanding the network" phase, crucial to obtain the necessary Joint Intelligence Preparation for Operational Environment (JIPOE) document. Secondly, the "identity intelligence" phase which relies on Human Intelligence (HUMINT) but now transfers the main role to Technical Exploitation (TE). And finally, the "Attack the network" phase, but not only from a kinetic perspective. We need to reach cognitive superiority acting across the multidomain.

Russian PMSCs

Focusing on Ukraine, we have to mention the so-called Wagner mutiny, which was nothing more than the stubbornness of a businessman, Y. Prigozhin, to subordinate himself to a ministerial level, regardless of his direct relations with Putin. The rest of Russian PMSCs (almost forty companies according to declarations from the Vice Minister of Defense Nikolai Pankov to Russian press) signed the contract with Russian government.

Although Russia is not a signatory nation of the Montreaux Document, focusing on the Geneva convention, its perspective is totally different. It not only signed the document, but it also perfected definitions and included it within its Constitution. After the latest legal modifications of the Russian criminal code, on 14th February 2024, it is impossible to organize an illegal military unit in Russian soil. Or at least, theoretically...



The demands of other markets, such as the various African nations where the attempt to acquire Wagner has failed, existing security contracts, and third-party actors (state or non-state) entering this new area of business have had to be considered secondary due to the evolving situation in Ukraine.

This was demonstrated by the fact that Africa Corps (Russian paramilitary group controlled by the government) withdrew from Ukraine during its initial expansion, followed by a "definitive" deployment to certain African countries.

According to Africa Corps' social media channels, the community manager had to cut some complaints from combatants about their destinations. Some voices claimed that, although they had signed a contract to serve in Africa, they were currently serving in Ukraine in contrast with Wagner PMC, that declares to be deployed only in Mali and Belarus.

Current situation

Until April 2025, Africa Corps was allowed to transfer combatants thanks to an existing contract with Russian MoD, as long as several conditions were met. The first and most important was not to be part of the so-called special operations in Ukraine. It seems that Russian MoD wants to maintain the whole available manpower just in case new fronts should be opened.

From a NATO perspective, is not possible to open a new front, but from a Russian perspective there are some cognitive actions, mainly disinformation campaigns claiming that the new NATO operation, Baltic Sentry, is a false argument to open a new front against Russia along the Baltic States.

Exaggeratedly, some Russian mass media have published that NATO would be committing piracy and the unique solution would be to hire armed guards to join the crew of the ships that navigate across the Baltic Sea. To sum up, this would turn into a new opportunity for PMSCs to be established near NATO Nations' boundaries.

Of course, officially, there are currently no PMSCs fighting in Ukraine, but when the Kremlin has a new need (for example, in an African nation), the 81st specialized volunteer brigade is removed from Ukraine and BEAR PMC appears where this new priority arises...

How the war is evolving in Ukraine is interesting from the point of view of development of new technologies or the evolution of existing Tactics, Techniques and Procedures (TTPs) that should likely be included in Russian doctrine and in NATO doctrine.

But we must not forget that in Belarus, Wagner PMC, the unique PMSC that presumably has not signed a contract with the Russian government, continues training the new units of the armed forces (mainly, special operations units), teaching in military academies and training (and of course, giving equipment) "GuardService", the only Private Military and Security Company allowed to have weapons.

Conclusions

A large number of Wagner activities are being conducted near three NATO boundaries, which means that at least three NATO nations could formally invoke article four of the North Atlantic Treaty.

In the long term, the questions to be answered are when the illegal aggression of Russia to Ukraine will reach a permanent cease of fire, and what is the expected future for all these PMSCs once the contract with the Russian government is extinguished?

The global market of explosive-laden drones: migration of Tactics, Techniques & Procedures from Ukraine to Africa

Unfortunately, and again, some of the prospectives estimated by the C-IED COE analysts have gone from analytical reports to evidenced reality: the explosive-laden drones have made their wide and full appearance in Africa.
The first reported cases had their origin in Libya, Central African Republic (CAR) and Mozambique.
Until early 2024, the use of Unmanned Aircraft Systems (UASs) by groups related to DAESH and Al Qaeda in Africa was merely limited to Intelligence, Surveillance and Reconnaissance (ISR), support to attacks (forward observer) and digital video recording platforms in benefit of further propaganda.

It was the activity of Russian Private Military Companies (PMCs) what initially brought the use of explosive-laden drones and barrel bombs to the Sahel area.
Logically, the forces of Jama'a Nusrat ul-Islam wa al-Muslimin (JNIM) copied those Tactics, Techniques and Procedures: first, dropping improvised munitions from commercial-off-the-shelf (COTS) drones and later, transforming First Person View (FPV) race UAS into Vehicle Borne Improvised Explosive Devices (VBIEDs).
With the Ukrainian Special Forces as suspected supporters, several attacks with UAS VBIED have been conducted in Sudan (e.g. simultaneous attack with 14 FPV VBIED against a convoy of Rapid Support Forces and Wagner fighters in Omdurman).

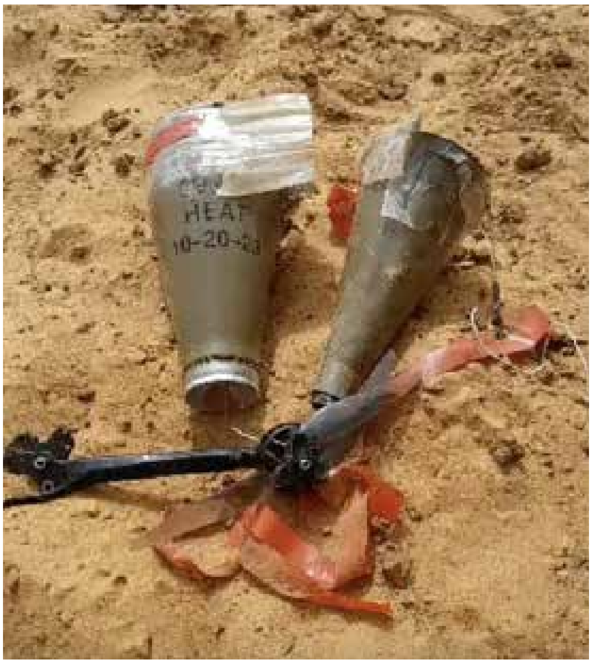
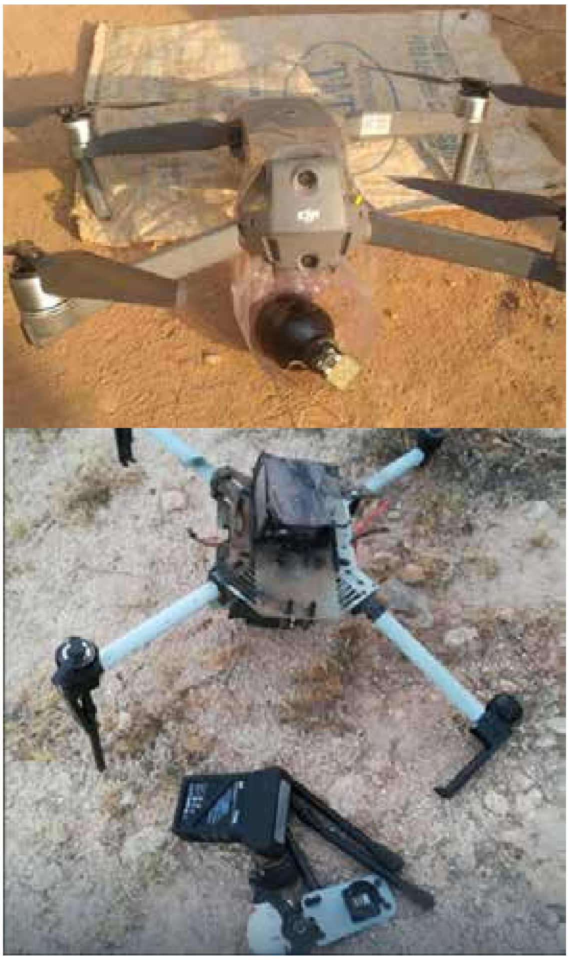


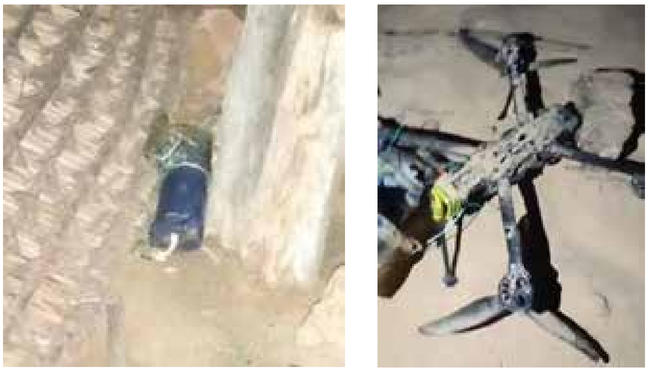
Figure 3 – Explosive-laden drone allegedly used by Wagner fighters in Anefis, Kidal MLI in October 2023 (Source – X)


Figures 1 and 2 – Explosive-laden drones reported in Central African Republic and Libya (Source – X, Telegram)

DAESH Somalia is widely utilizing FPV race explosive-laden drones in Puntland, Somalia, since 2024, which could be worrying due to the presence of foreign fighters among their forces.

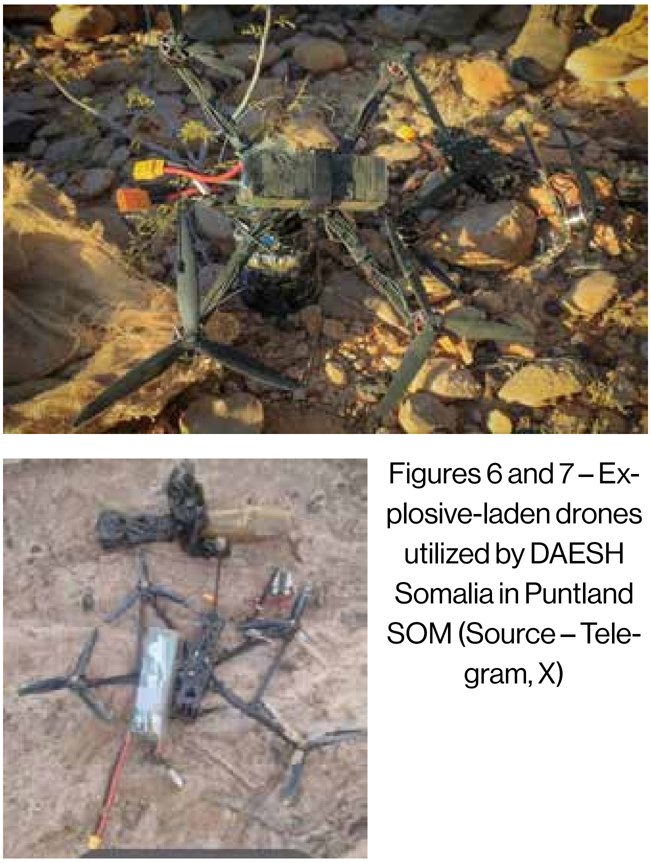
As unfortunately expected, the migration of the use of explosive-laden drones has also taken place in the areas controlled by DAESH in West Africa Wilayat (ISWAP), especially Nigeria and Chad, usually in the form of improvised munitions being dropped from COTS UAS (notice the release systems in figures 8 and 9).

On the other hand, Nigerian troops have been suffering from the use of drones by other violent groups apart from ISWAP. A UAS manufacturing factory operated by armed fighters of the Eastern Security Network (ESN) (as militant branch of the Indigenous People of Biafra (IPOB)) was reported in Onicha Ulona, South local government area of Delta State, Nigeria, in March 2024.

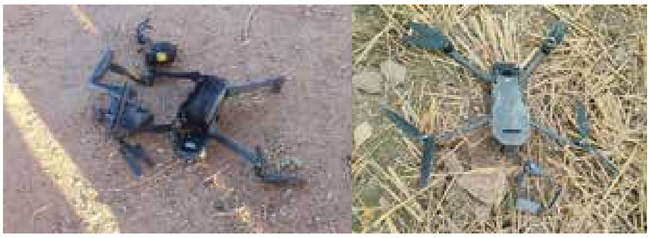


Figures 4 and 5 – Samples of explosive-laden drones used by JNIM (Source – X)

Again, and due to the lack of information security and exaggerated exhibit of military activities, the Ukrainian theatre of operations is posing a bad example to follow by non-state actors.



Figures 6 and 7 – Explosive-laden drones utilized by DAESH Somalia in Puntland SOM (Source – Telegram, X)



Figures 8 and 9 – Pictures of ISWAP explosive-laden drones taken in Nigeria and Lake Chad Basin (Source –X)

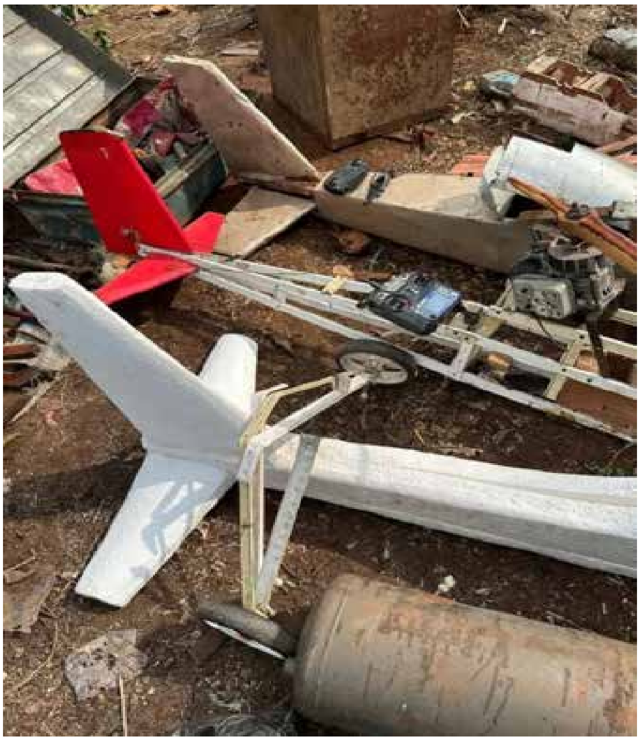


Figure 10 – Drone manufacturing factory of IPOB/ ESN in Nigeria (Source – www.goldenpage.ng)

Death could be a matter of proximity: proliferation of victim operated switches in Ukraine

During the conflict in Ukraine, everyone was expecting the typical wide use of “boobytraps” (basic field versions of Victim Operated Improvised Explosive Devices (VOIED)), as described in Russian tactical doctrine.

Accordingly, and from the very first phases of the conflict originated in 2014, we witnessed the use of those rudimentary IEDs, mainly based on slightly manipulated hand grenades (e.g. weakened safety pin) or other conventional or manipulated munitions associated with improvised or officially issued initiation devices.
Along with the tactical manipulation of hand grenades, the mutual knowledge about the adversary Tactics, Techniques and Procedures (TTP) regarding mine clearance has led to the transformation of conventional landmines into VOIED in the aim of making their defusal, recovery and/or lifting much more complicated to the Combat Engineer elements.

The different procedures for countering the mine clearance have evolved progressively in the Ukrainian theatre of operations, passing through the different steps below:

- Emplacement of associated pressure release systems behind or beside the landmine.
- Manipulation of the landmine fuzes to avoid their removal aiming to recover the munition:

  -Mechanical pyrotechnic switches.
  -Mechanical-electrical switches.
  -Electrical switches (e.g. light-sensitive devic es, presence detectors...).
  -Chemical initiation (e.g. pouring homemade liquid explosive which would progressively evaporate and recrystallize around the fuze).
- Improvised copies or versions of scatterable munitions including victim operated switches.

As an example, one of the most widely trapped landmines has been the different versions of MON-50 (MOH-50) anti-personnel directional fragmentation (APDF). Their main TTP consists of removing the detonator from the landmine body once discovered, as a huge variety of mechanical-electrical systems have been emplaced inside those landmines in the aim of closing an electrical circuit when the detonator is extracted.
But the most worrying design for victim operated switches used in Ukraine is based on the updates both parts of the conflict made to the Ukrainian-made “Джони” (Jhonny) microcontrollers.
While Ukraine has developed the “Dzhonik” and “Verba” electronic devices, Russia has also developed their own version under the denomination “MAG-3”.

That kind of microcontrollers contain all or some of the following features:

- Magnetic influence switch.

ЗАПАЛ УЗРГМ РУЧНОЙ ГРАНАТЫ Ф-1(РГД-5)

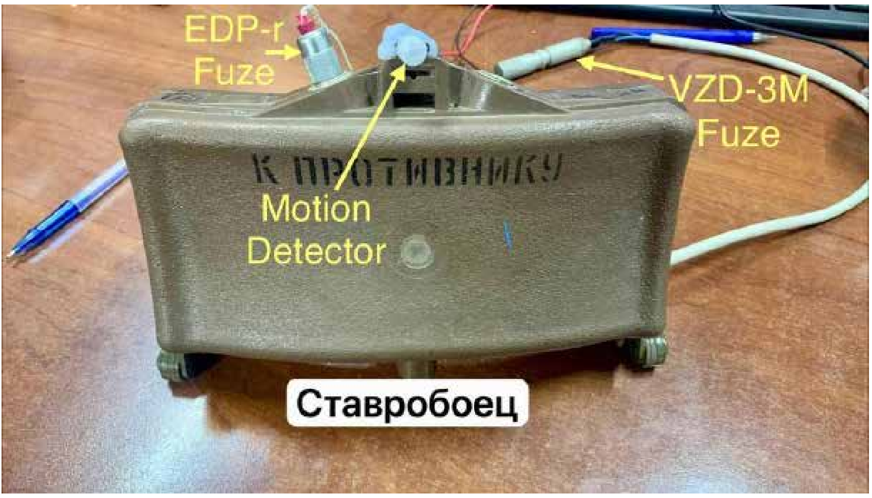
Figures 1, 2 and 3 – Pages from a Russian handbook on the improvised use of hand grenades (Source – VKontakte, Telegram)

- Anti-movement through an electronic accelerometer.
- Impact activation.
- Time delay.
- Radio control.
- Battery expiring initiation.

Lately Ukrainians have developed a doppler-effect based motion detection version of the microcontrollers, which is providing the same antihandling capability through microwaves.

In fact, the reports from Ukraine evidence the high effectiveness of those microcontrollers in getting activated with the proximity of the first responders.

Regarding the distance of activation in magnetic



Разминирование «Подарочков» после свино собак (Напоминаю при обнаружении мин,В/У не в коем случае не прикасайтесь к ним, это смертельно опасно!!!!!!!). Слава Украине

Figures 4 and 5 – Some VOIED modifications over MON-50 landmines in Ukraine (Source – TikTok, X, Reddit)

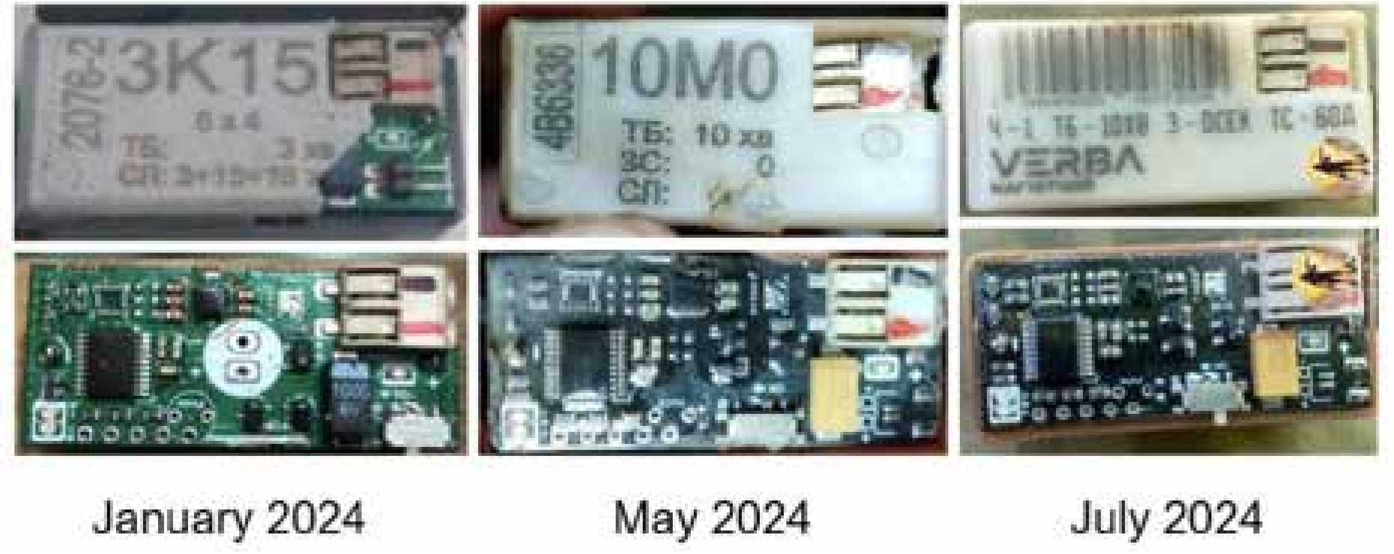
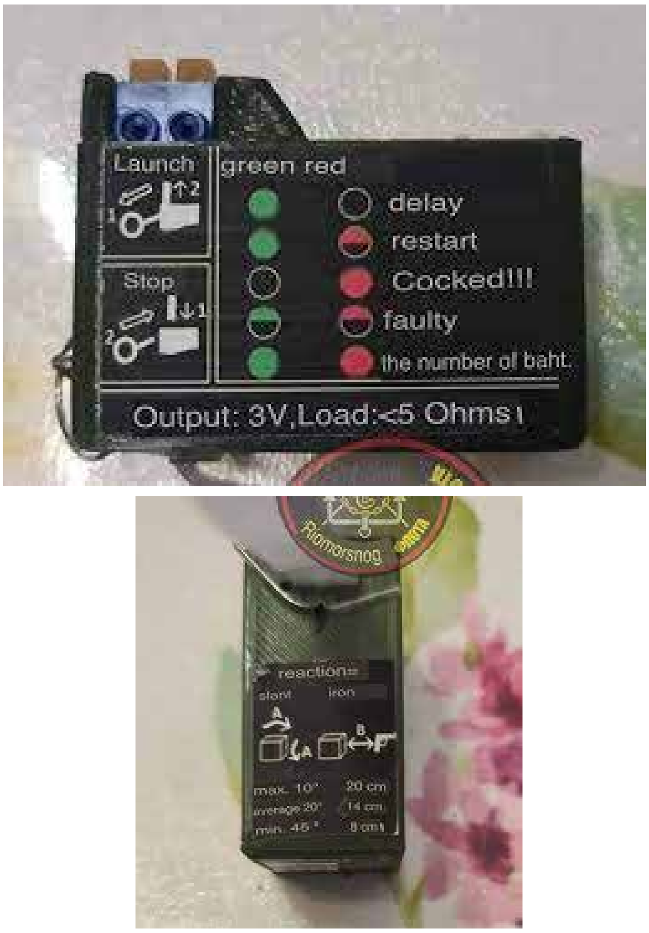


Figure 6 – Ukrainian Джони-M (Jhonny-M), x Джони -K (Jhonny-K) and Verba electronic devices (Source – Telegram)

influence mode, it depends on the metallic mass, which could be activated when a military vehicle is approaching.

They are mostly using CR123A 3V battery: in a passive usage, such as this kind of VOIED switch, the service life can be more than a year with the right conditions. This would turn the IEDs connected to those micro-controllers into a high risk for civilians after the end of the conflict.

On the other hand, their recognition and detection in critical infrastructures like international airports would be really hard, as well as a part of VOIEDs in an urban environment.



Figures 7 and 8 – Russian “MAG-3” microcontroller (Source – X, Telegram)

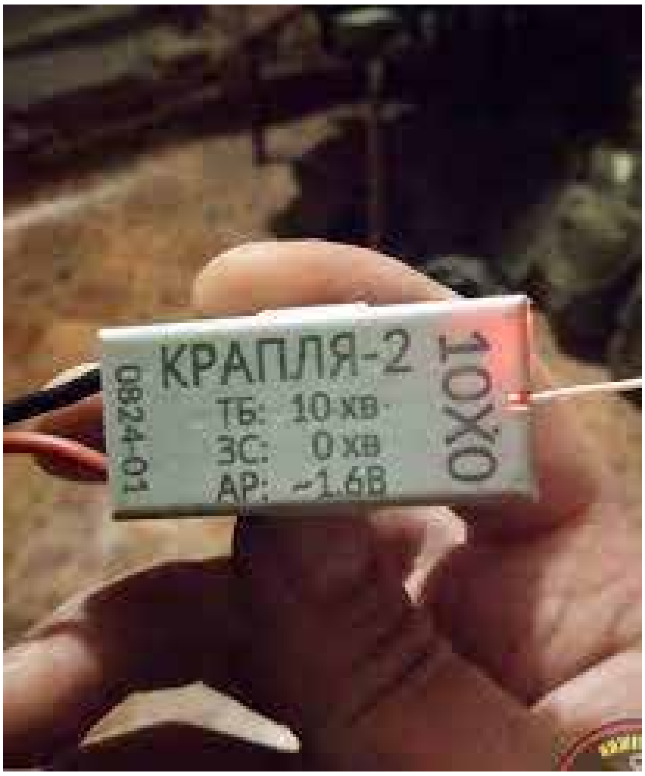
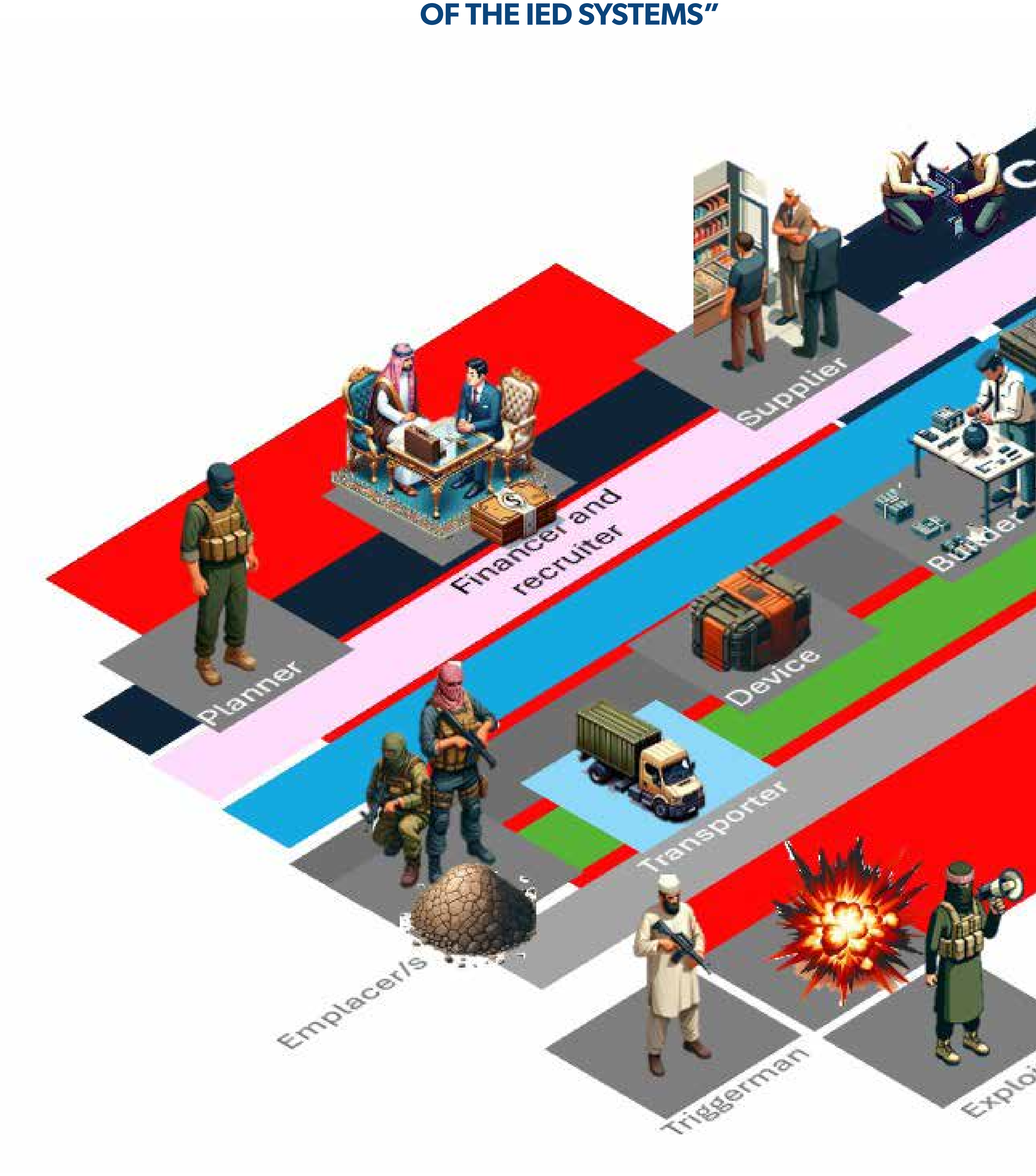
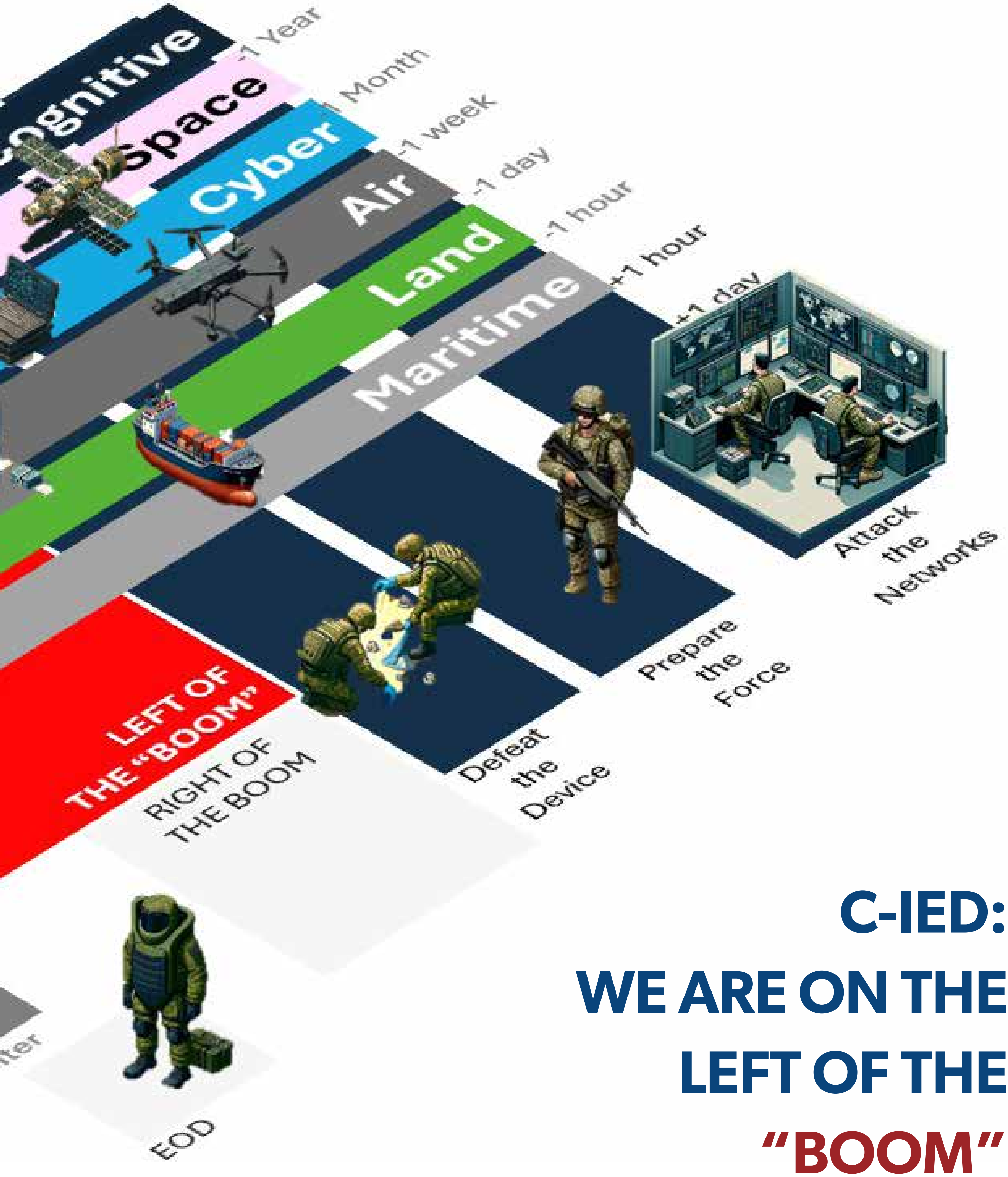


Figure 9 – Ukrainian ›КРАПЛЯ‹-2 “DROP-2” doppler radar motion detection microcontroller (Source – X, Telegram)

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"

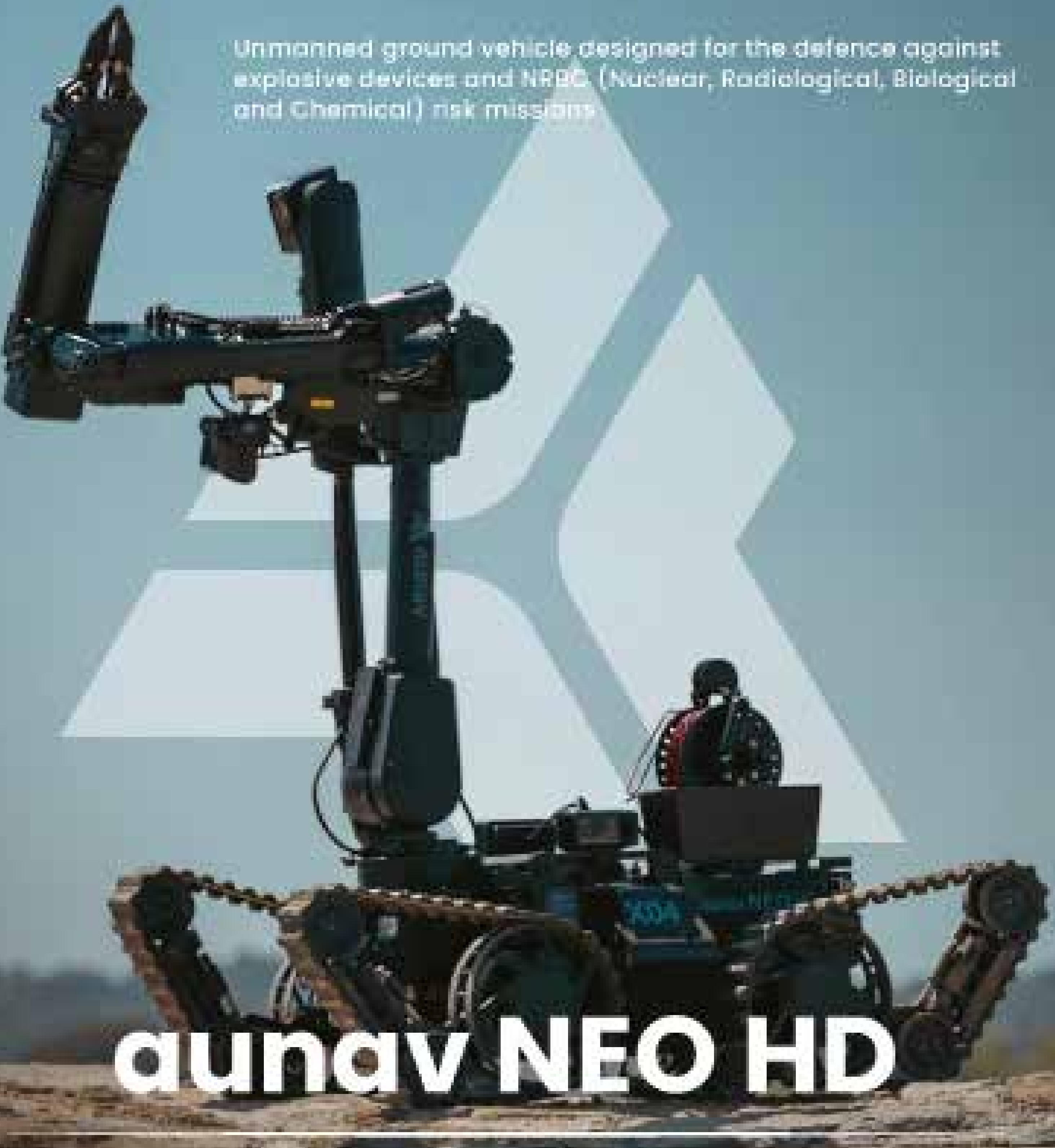




C-IED: WE ARE ON THE LEFT OF THE "BOOM"

em&e group

Unmanned ground vehicle designed for the defence against explosive devices and NRBC (Nuclear, Radiological, Biological and Chemical) risk missions



aunav NEO HD

- Light and compact
- Its width can be increased or decreased thanks to its variable geometry system
- Adaptable to multiple scenarios

WWW.EME-ES.COM

A New Paradigm in Lessons Learned: What NATO Can Learn from Ukraine

It is widely recognized that NATO possesses a sound and robust Lessons Learned (LL) concept. This framework is built upon a well-established doctrine. However, upon closer inspection, one notices a notable omission: while the doctrine speaks at length about being a learning organization and outlines how learning should occur, it never defines the precise scope of formal learning.

In our view, this ambiguity has led to the LL process being applied to matters for which it was never intended. Therefore, for the purpose of this article, let us clarify from the outset: Lessons Learned should apply exclusively to the review and improvement of formal processes, typically expressed through Standard Operating Procedures (SOPs), doctrine, guidance, handbooks, and Tactics, Techniques and Procedures (TTPs). It is in these areas that the LL process can reveal its full potential.

Other issues-such as decision-making errors or mistakes in execution-should certainly be subjected to critical analysis, but there are more suitable mechanisms for doing so, such as debriefings and quality assurance processes.

For those unfamiliar with NATO's LL process, it currently relies on a tool that, while imperfect, is already in the process of being replaced by a more modern and effective alternative. The system may appear rigid and cumbersome at times, but this also makes it relatively robust and fail-safe.

A Lesson from Ukraine

So, why does the title of this article suggest that the war in Ukraine presents a new paradigm from which we should learn? Let us begin from the beginning.

The first time we encountered how the Armed Forces of Ukraine (AFU) were managing LL was at the Annual Lessons Learned Conference in Lisbon, nearly a year ago. There, the Boryviter Centre of Excellence-a non-profit volunteer organization founded in April 2022 to support the AFU's training efforts-delivered a presentation that left a lasting impression.

One of Boryviter's major initiatives was the development of a new LL system, as the AFU's pre-war structure quickly became obsolete in the face of fast-paced operations and limited resources. The old system was simply too slow and inflexible; even when lessons were identified, they could not be translated into timely feedback for training or frontline operations.

Boryviter took a fresh, adaptive approach. Using NATO's LL doctrine as a starting point, they created a solution tailored to the operational reality on the ground. On paper, the system was impressive: it relied on a secure smartphone application, available to troops in the field. It was designed to be simple enough so that even the busiest or most inexperienced officer and NCO could use it. Beyond collecting observations, the system also gathered After Action Reports (AARs) from the lowest tactical levels and used Artificial Intelligence to analyze data and translate plain-language inputs into structured military reporting formats.

The concept appeared both innovative and pragmatic.

Field Realities and Cultural Resistance

In February, during the AFU's annual LL conference in Kyiv-attended virtually by the C-IED COE-we heard firsthand accounts from frontline commanders. From them, we learned that the AFU had, from early on, employed encrypted commercial apps like Signal to share experiences and best practices. This ad hoc system fostered trust-based networks among veteran units. However, it also created isolated "bubbles of confidence," where younger or less experienced units were unable to benefit from hard-earned lessons, and the army at large struggled to incorporate battlefield insights into formal training and doctrine.

When Boryviter's formal system was introduced, frontline units were reluctant to adopt it. Having invested trust and time in their informal methods, they viewed the new system as an administrative burden with little return and no visible feedback loop.

Our conclusion after attending both conferences is that the AFU currently operates with an informal, decentralized LL system that is effective in spreading best practices among some units and even influencing training at times, but it remains limited in its ability to impact formal doctrine. Whether Boryviter's system will ultimately be embraced remains an open question.

What NATO Can Learn

What lessons can NATO draw from this experience?

As stated at the outset, NATO's current LL process is conceptually sound and should be preserved. It provides critical capability in tracking and amending doc-

trinal documents, something the AFU's system lacks.

However, it is equally clear that, in a high-intensity conflict, NATO would likely face the same constraints the AFU encountered. Therefore, NATO should consider developing a parallel LL system, one that complements the existing process and is designed to deliver flexibility and rapid feedback to tactical units. Such a tool could capture frontline observations and best practices in real time while still channeling them-when appropriate-into the broader LL architecture.

Implementing such a tool will not be easy. Its scope, hardware requirements, security protocols, and balance between field usability and data protection must be studied in detail. Fortunately, Ukraine's experience provides a valuable foundation.

But even the best-designed system will fail if users are unprepared or unwilling to adopt it. That is why integration into peacetime training is critical. A tactical LL system must become second nature to junior leaders and routinely used during field exercises. Otherwise, we risk repeating the AFU's implementation struggles.

The C-IED Perspective

Some may question whether a new tactical LL system is truly necessary. In the C-IED approach, however, the need is clear. During the Afghanistan campaign, many nations resorted to local systems to collect and share TTPs, but these often stayed within national units, leaving others unaware and unprotected.
While NATO has effective channels for sharing IED-related intelligence, these are not designed to

analyze or improve our own operational behavior. For that, a tactical LL tool-integrated into the "Prepare the Force" pillar-would be immensely beneficial.

Conclusion

When Russia invaded Ukraine, the AFU had to rapidly develop new mechanisms to circulate TTPs and best practices across a constantly shifting battlefield. Their informal solutions were innovative and effective, but now face institutional barriers to long-term adoption.

NATO has the advantage of time and foresight. We can begin now to design and integrate a complementary LL process—agile, field-ready, and doctrinally connected—before the need becomes urgent.

In doing so, we not only strengthen our learning capacity but also ensure that lessons, once paid for in blood, are never forgotten.

The C-IED approach in the light of NATO Warfare Development Imperatives

The NATO Warfighting Capstone Concept provides five warfare development imperatives to focus and synchronize efforts to develop the Alliance Military Instrument of Power (MIoP).

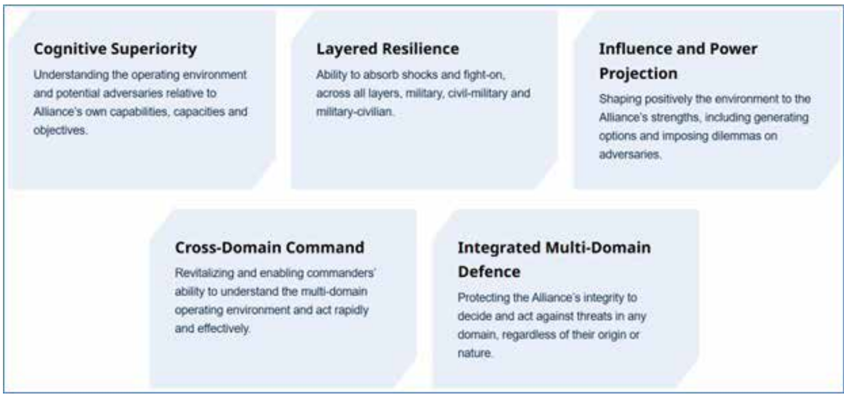
One of those imperatives is **“Cognitive Superiority”** (COGSUP), which is described as the degree of dominance through possessing and applying faster, deeper and broader understanding and more effective decision-making than adversaries.

From a C-IED perspective, the blocks derived from the concept for Cognitive Superiority have always been considered from the Attack the Networks approach:

- Awareness (sensing) is essential for deep knowledge about the threat, our own capabilities and the Human Terrain through analyzing the cognitive environment.
- Understanding (sense making) poses a must for Human Network Analysis and Support to Targeting/Engagement.
- Advantage (acting) fully implies Human Network Engagement and Assessment steps.

Nonetheless, the main problems for an effective and anticipatory application of the C-IED approach (Attack the Networks) remain active for achieving the Cognitive Superiority: information collection and intelligence processing capabilities need to be reinforced, enhanced, and refined. This, in general terms, has never happened even from the Allied implication in Afghanistan, Iraq and other conflicts. The emerging threat scenarios unavoidably require an increase in intelligence capabilities and an evolution of the processes associated with those intelligence capabilities.

On the other hand, the development of Allied initiatives in the field of Cognitive Warfare (COGWAR) is directly associated with a Cognitive Superiority imperative: from an Attack the Networks point of view, the current approach to Cognitive Warfare has been considered inside the always essential-to-success non-lethal actions.



Cognitive Superiority
Understanding the operating environment and potential adversaries relative to Alliance's own capabilities, capacities and objectives.

Layered Resilience
Ability to absorb shocks and fight-on, across all layers, military, civil-military and military-civilian.

Influence and Power Projection
Shaping positively the environment to the Alliance's strengths, including generating options and imposing dilemmas on adversaries.

Cross-Domain Command
Revitalizing and enabling commanders' ability to understand the multi-domain operating environment and act rapidly and effectively.

Integrated Multi-Domain Defence
Protecting the Alliance's integrity to decide and act against threats in any domain, regardless of their origin or nature.

Figure 1 – NATO warfare development imperatives (Source – www.nato.int)

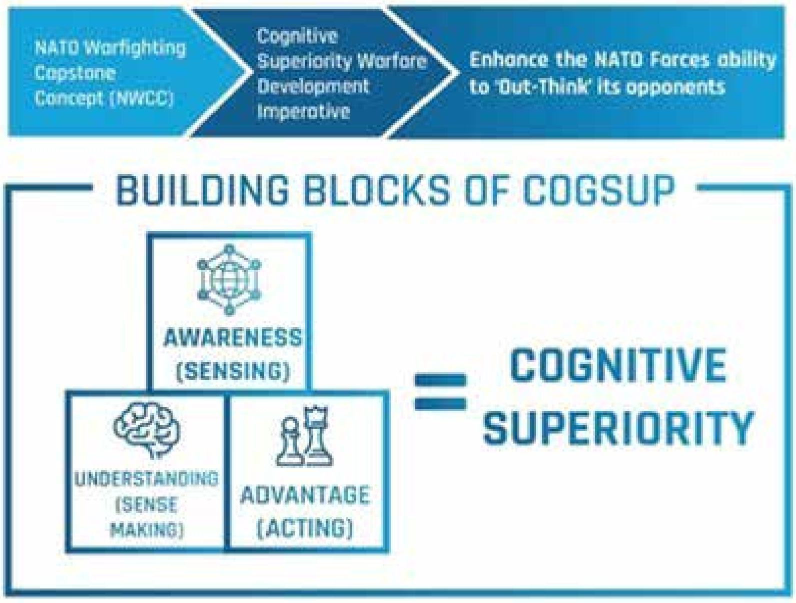

NATO Warfighting Capstone Concept (NWCC)
Cognitive Superiority Warfare Development Imperative
Enhance the NATO Forces ability to 'Out-Think' its opponents
BUILDING BLOCKS OF COGSUP
AWARENESS (SENSING)
UNDERSTANDING (SENSE MAKING)
ADVANTAGE (ACTING)
=
COGNITIVE SUPERIORITY

Figure 2 – NATO description of Cognitive Superiority (Source – www.nato.int)

COGWAR integrates cyber, information, psychological and social engineering capabilities. These activities, conducted in synchronization with other instruments of power (not only the MIoP), can affect attitudes and behaviours by influencing, protecting or disrupting individual and group cognition to gain advantage over an adversary. In fact, there is a huge umbrella of different Emerging and Disruptive Technologies (EDTs) which could potentially support COGWAR development.

With regards to **“Layered Resilience”,** a sort of comprehensive and holistic approach to collective defence resilience, it would refer to the ability of a single nation and all Allied nations to withstand and recover from a broad spectrum of threats and challenges.

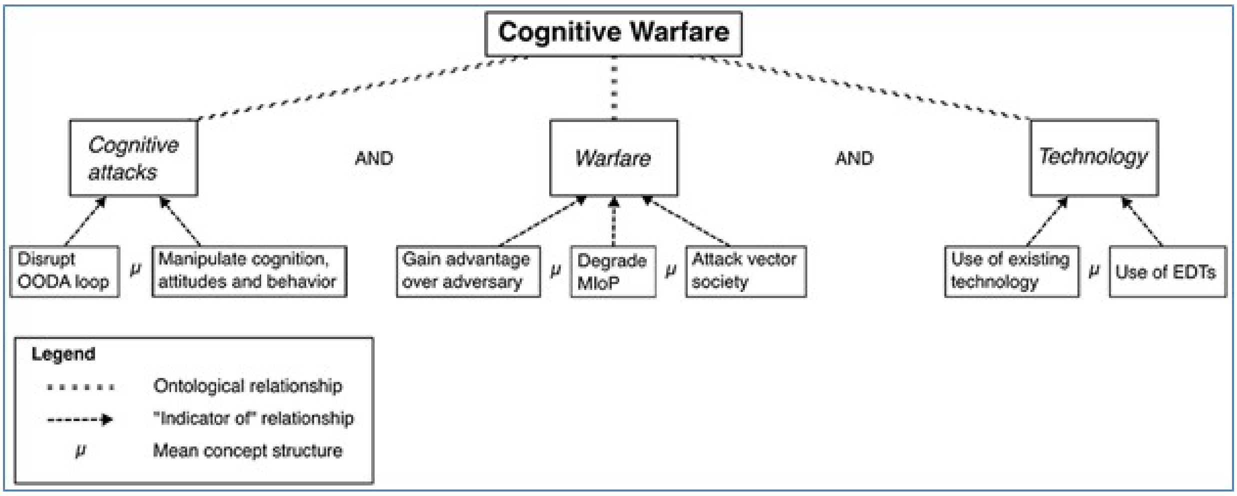


Figure 3 – Visualization of NATO Cognitive Warfare working definition. (Source - https://doi.org/10.3389/fdata.2024.1452129)

Accordingly, NATO emphasizes that the resilience of each member country contributes to the overall strength and preparedness of the Alliance, but the common cohesion and unity of effort are also essential.

Although a layered resilience is not directly related to a generic C-IED approach, it is partially applicable from an Attack the Networks perspective when referring to both:

- The preparation of friendly human networks against the potential negative effects from adversary actions.
- The effectiveness of our own actions carried out to achieve positive effects over friendly human networks in the benefit of strengthening our own capabilities to undermine the potential development of adversary capabilities.

From the combination of the other three imperatives (**"Influence and Power Projection", "Cross-Domain Command"** & **"Integrated Multidomain Defence"**) we could fall upon the Allied implementation of the concept for Multi-Domain Operations.

Multidomain Operations (MDO) is currently defined by NATO as "the orchestration of military activities, across all domains and environments, synchronized with nonmilitary activities, to enable the Alliance to deliver converging effects at the speed of relevance".

After an initial review, MDO concept is mostly based on:

- Military and nonmilitary activities synchronization, which is another way of considering the essential "Interagency" flavour of C-IED/Attack the Networks.
- Actions over all domains and environments, which has been a must for C-IED/Attack the Networks from its conceptual creation.
- Integration of effects at the speed of relevance, which is the root of the application of C-IED/Attack the Networks approach to affect the capabilities of human networks.

In conclusion, it seems that the MDO approach is already implemented (fully applicable to C-IED) into the Attack the Networks approach from its very beginning in 2008. Along with the evolution of the emerging threats and the persistence of IEDs as future weapons of choice, we can affirm that C-IED is still valid and necessary.

References

(NATO) 2019 NATO Military Strategy

(NATO) 2020 Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA)

(NATO) 2021 NATO Warfighting Capstone Concept (NWCC)

(NATO) 2022 NATO Warfare Development Agenda (WDA)

(NATO) 2022 NATO Strategic Concept

(NATO) 2024 Secretary General's Annual Report

www.e-arc.ro

www.irsem.fr

www.japcc.org

www.tandfonline.com/journals/ucst20

www.c2coe.org

www.act.nato.int

www.finabel.org

www.cssas.unap.ro

INERT PRODUCTS, LLC
INERT EXPLOSIVE TRAINING PRODUCTS

Inert Products LLC
US Based Defense Company

703 Hudson Ave
Scranton, PA, USA 18504

+1 570 341 3751 ☎
info@inertproducts.com ✉
www.inertproducts.com

UGV

#1 Cost-Effective UGV for EOD and Demining Operations

R-BOT

Designed for durability, the R-BOT showcases exceptional operational capabilities in the most challenging environments. The R-Bot has been operationally proven to handle landmines, UXO, IEDs, booby trapped land mines, and downed drones weighing up to 44 lbs (20kg).

CBRNe

Chem/Bio Training Aids

EOD

EOD/C-IED Training Aids

Inert Products, LLC is the leading manufacturer of high-quality EOD and CBRNe training products designed for realistic hands-on training. Since 2007, we've supported military units around the globe with replica ordnance, IED training kits, EOD robots, and CWA simulants.

WWW.INERTPRODUCTS.COM

C-IED COE project: AMATE, a 21st Century alternative to CARVER

From a C-IED Attack the Networks perspective, the Target System Analysis (TSA) poses an essential process: its aim is to determine enemy vulnerabilities and exploitable weaknesses, along with what effects will likely be achieved against target systems and their associated activities. But TSA is simultaneously a systematic approach, a product and a process. As a process, TSA entails identifying, describing and evaluating the composition of an adversary target system to determine its capabilities, requirements and vulnerabilities.

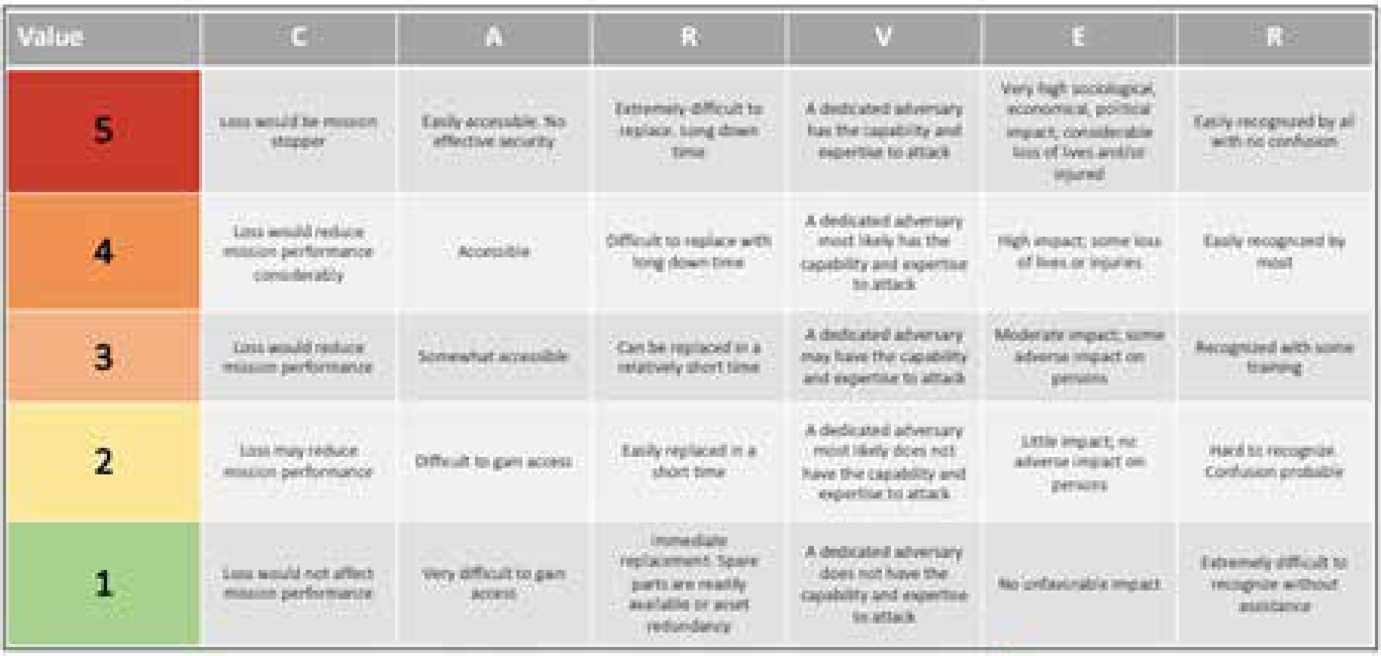
But there is a problem: current TSA was air force-centric, designed for targeting conventional forces, so it is not too much applicable to adversary non-state actors nor is it useful for neutral or friendly human networks at all, as they are not considered inside the Targeting process (see the currently approved version of AJP-3.9 Allied Joint Doctrine for Joint Targeting).
Additionally, there are not developed procedures for TSA on human networks or any effective scientific approach to it. Therefore, all the efforts and responsibility must lay on the analysts themselves, just based on individual intellect, experience, imagination... and for sure also personal or collective bias.

As an example, we could analyze the most typical methodologies for analysis and prioritization of targets:

- CARVER (Criticality, Accessibility, Recoverability, Vulnerability, Effect and Recognizability)
- BARRIL (Benefit, Accessibility, Replaceable, Reconcilable, Influence and Leverage)

In fact, CARVER was developed during the Second World War as a quantifiable method to select targets in support to the agents working with the resistance inside the territory occupied by Germany. It was refined during the Vietnam War and it is still used as a methodology for target analysis and vulnerability assessment.
Both CARVER and BARRIL don't take into account enough criteria to absorb bias or mistakes, and the assignation of values is too subjective, confusing and unclear, which could make the result vary depending on the analyst.

Nonetheless, CARVER is more useful for vulnerability assessment, and it was designed for conventional targets and lethal actions, which makes it not quite adequate for non-state actors.



Value	C	A	R	V	E	R
5	Loss would be mission stopper	Easily accessible. No effective security	Extremely difficult to replace. Long down time	A dedicated adversary has the capability and expertise to attack	Very high sociological, economical, political impact, considerable loss of lives and/or injured	Easily recognized by all with no confusion
4	Loss would reduce mission performance considerably	Accessible	Difficult to replace with long down time	A dedicated adversary most likely has the capability and expertise to attack	High impact; some loss of lives or injuries	Easily recognized by most
3	Loss would reduce mission performance	Somewhat accessible	Can be replaced in a relatively short time	A dedicated adversary may have the capability and expertise to attack	Moderate impact; some adverse impact on persons	Recognized with some training
2	Loss may reduce mission performance	Difficult to gain access	Easily replaced in a short time	A dedicated adversary most likely does not have the capability and expertise to attack	Little impact, no adverse impact on persons	Hard to recognize. Confusion probable
1	Loss would not affect mission performance	Very difficult to gain access	Immediate replacement. Spare parts are readily available or asset redundancy	A dedicated adversary does not have the capability and expertise to attack	No unfavorable impact	Extremely difficult to recognize without assistance

Figure 1 – CARVER matrix (Source – www.smiconsultancy.com)

Although there are some generic references and definitions inside military doctrine, we are still missing a specific and standardized procedure for Target System Analysis on non-state actors, which are very different from those conventional forces for which our TSA procedures were designed time ago.

Additionally, and based on both its structural and scientific limitations, the traditional CARVER methodology does not adequately cover the needs for target/audience selection and prioritization on non-state actors and other human networks. Although it still works for vulnerability assessment, CARVER is about eighty years old and too lethally oriented.

Accordingly, a modern and effective Attack the Networks approach would need an alternative updated tool for target/audience selection and prioritization. In order to achieve it, we should not only focus on the characteristics of the target itself, but also on the actions to conduct and the effects to achieve.

That is why the C-IED COE Attack the Networks branch has developed a new approach to the prioritization of targets and audiences. In the aim of increasing the scientific approach and objectivity of the analysis, the number of criteria is increased to fifteenth (instead of the six from CARVER), and their respective quantification through values (1-5) is intended to be clearly and accurately defined.

In that way, the proposed criteria are as follows:

- (Related to TARGET) Reactivity, Sensitivity, Identification, Counter Measures & Resistance.

- (Related to ACTION) Easy, Cost-Effective, Foreseeable, Surgical & Attribution.

- (Related to EFFECT) Exploitability, Persistence, Evaluability, Sinergy & Impact.

Additionally, the C-IED COE has developed a calculator tool for AMATE, and it is even applying the AMATE methodology during the two-week NATO Attack the Networks Operational Course (ATNOC), which is conducted twice a year by the C-IED Centre of Excellence.

The 21st Century needs updated solutions for those problems deriving from new threat scenarios and evolving adversary human networks and this is the challenge for Attack the Networks.

Only if we are successful developing advanced analytical tools specifically adapted to non-state actors, instead of those designed for conventional forces, will there be an opportunity to anticipate and face the threats from violent extremist organizations.

Maybe these Attack the Networks initiatives to develop human network characterization, procedures on Target System Analysis for non-state actors, refined methodology for target/audience selection and prioritization could look like a chimera, but little by little, they are becoming draft documents which eventually could become handbooks or manuals. We may see the outputs in the close future.

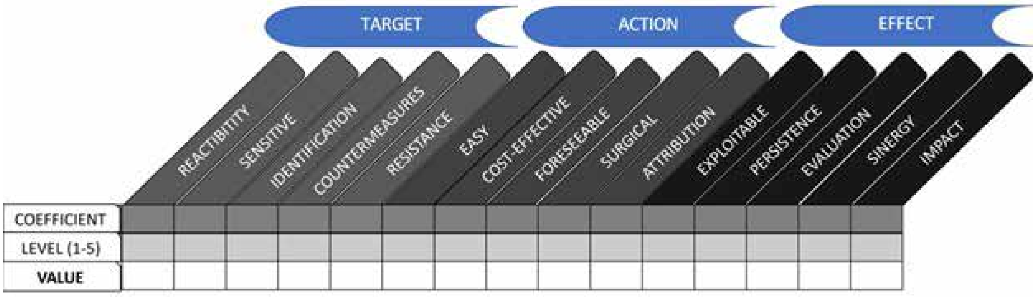


Figure 2 –Attack the Networks proposed model for selection & prioritization of targets/audiences (Source –C-IED COE)

References

C-IED COE (2024) - Handbook on Attack the Networks Procedures for Support to Effects and Target System Analysis over Non-state Actors and other Human Networks.

Counter-IED Report – Edition Autumn 2023 (2023) - "Targeting the Unknown": Human Network Characterization and Target Analysis Methodologies for a new Century".

CLARK R.M. (2022) - "Intelligence Analysis: A Target-Centric Approach". CQ Press.

CURTIS E. PINNIX, JR (2021) - "Specialized Analytic and Targeting Study. A Methodology and Approach for Conducting Faster Full-Spectrum Targeting" (Joint Force Quarterly 103). National Defense University Press.

MITCHELL T.E. (2020) - "Forging the Center of Gravity". Marine Corps gazette.

NATO STANDARD (2021) - "AJP-3.9 Allied Joint Doctrine for Joint Targeting". NATO Standardization Office (NSO).

Latest C-IED COE reports including those related to Ukraine, Russia and Wagner

1. **Ukraine – Manual on modification of conventional munitions for explosive-laden drones**
Describes adaptations made by Ukrainian forces or adversaries to repurpose munitions for drone delivery.

2. **Russian handbook on explosive-laden FPV drones**
Analyzes Russian techniques using First Person View drones as offensive platforms.

3. **Explosively Formed Penetrators (EFP) for First Person View (FPV) drones in Ukraine**
Covers a new trend involving the use of EFPs mounted on FPV drones in the Ukrainian conflict.

4. **Russian handbook on improvised TTPs with hand grenades**
Describes the tactical field use of grenades by Russian forces in irregular engagements.

5. **Russian TELEGRAM sharing online instructions for explosive manufacture**
Monitors Russian-language Telegram channels distributing bomb-making knowledge.

6. **Pro-Russian handbook on insurgency tactics**
Provides insights into materials promoting hybrid warfare and irregular tactics.

7. **Dynamics on Wagner Group's role in Africa and Ukraine**
Analyzes the operational footprint of Wagner in both regions and its adaptation of C-IED-relevant methods.

8. **Implications from Wagner Group training support to Belarus (BLR)**
Examines the export of Wagner's expertise into Belarusian security structures.

9. **Wagner Group Ground Force Commander**
Profiles key leadership figures within Wagner's operational chain of command.

10. **Wagner Group Access strategies to areas of operations**
Covers methods Wagner uses to gain ground access, influence and positioning in key theatres.

11. **Wagner Group as a global actor**
Outlines Wagner's multinational reach, tactics and influence mechanisms.

12. **Wagner Group Training and Recruitment**
Focuses on how Wagner sources, trains and deploys personnel.

13. **Wagner Group Splitting**
Reports internal divisions within Wagner post-Prigozhin and their operational consequences.

14. **Russian improvised passive protection/mitigation measures on airplanes against explosive-laden drones**
Describes makeshift defenses implemented on Russian aircraft in conflict zones.

15. **Russian AI-enabled explosive-laden FPV-drones**
Describes AI-supported FPV drones like the OVOD-S used by Russian forces for autonomous targeting and resistant to EW countermeasures.

16. **ISWAP use of explosive-laden drones**
Tracks the migration of explosive drone TTPs from Ukraine to West African groups like ISWAP and JNIM.

17. **DAESH Threats against Europe 2024-2025**
Reviews DAESH-linked plots and threats in Europe. Highlights IS-KP's transnational operations including Russia and Ukraine.

18. **LAMANHO group delay detonator manual**
Describes how a pro-DAESH Chechen group disseminates Russian-language manuals on homemade delay detonators, posing risks of replication in extremist circles.

19. **DAESH Threats against Europe 2024-2025 (Update)**
Confirms persistent DAESH/IS-KP threats in Europe, with Russian and Ukrainian vectors noted in logistics and targets.

20. **Technical Exploitation on GERAN-2 UAS Warheads**
Analyzes different warhead types on Russian GERAN-2 drones, sourced from leaked Ukrainian intelligence.

21. **Houthi Leadership**
Reviews the leadership of the Houthi movement with emphasis on links to Iran and involvement in conflicts including deployment of personnel to Ukraine.

22. **Russian Handbook on UAS Chemical Improvised Munitions**
Shows how a leaked Russian handbook explains the potential use of chemical substances as main charge of improvised munitions for drones.

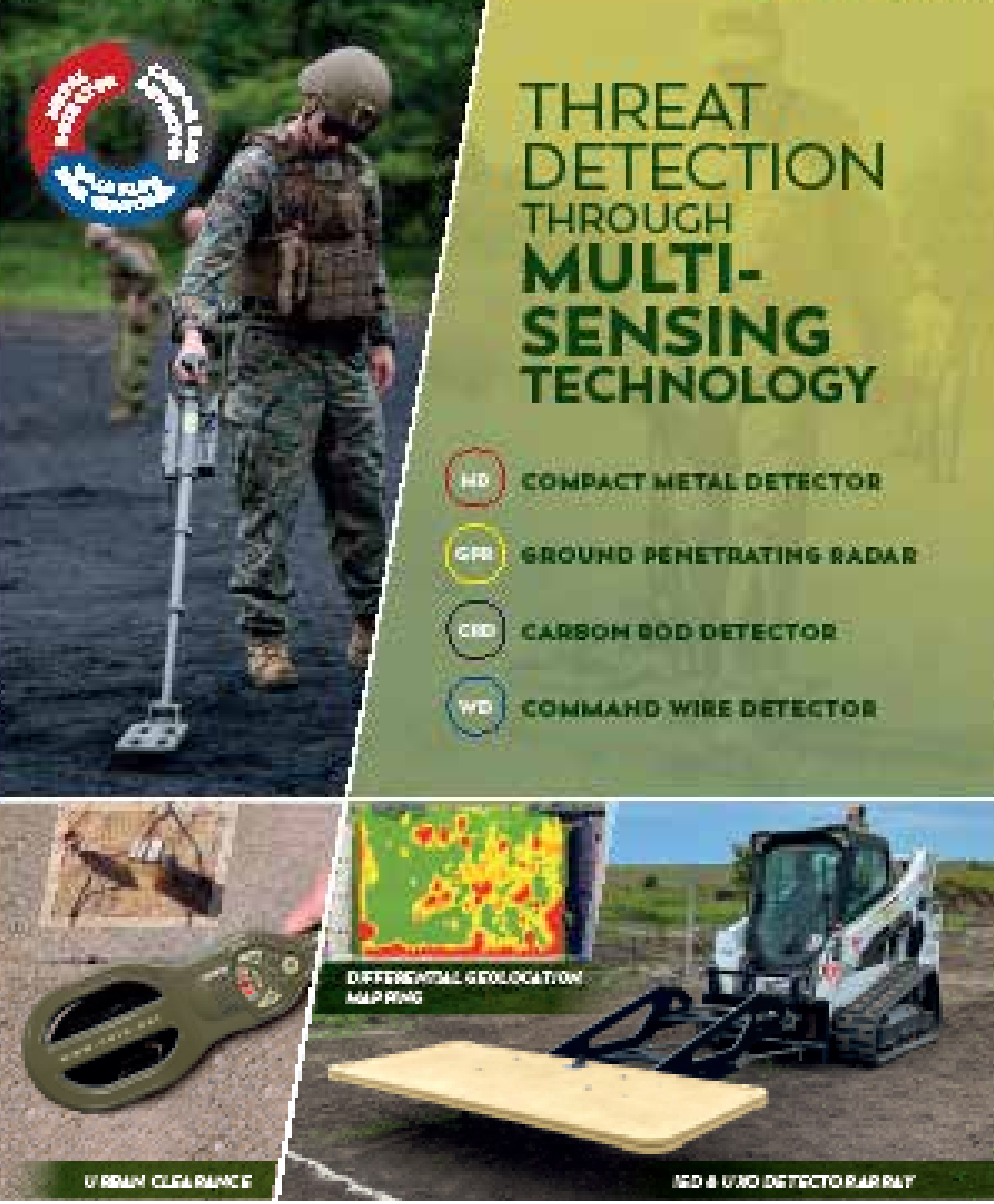
23. **JNIM capabilities**
Analyzes a document from a Russian Private Military Company in Mali about the military capabilities of Jama'a Nusrat ul-Islam wa al-Muslimin, including IED.

24. **Houthi Financing**
Details how Ansar Allah, the Houthi rebels in Yemen, have developed an intricated financial system to feed their needs of weaponry.

25. **Russian improvised passive protection/mitigation measures on submarines and oil refineries against explosive-laden drones**
Describes makeshift defenses implemented on Russian submarines and oil refineries in conflict zones.

These reports have been published through 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



THREAT DETECTION THROUGH MULTI-SENSING TECHNOLOGY

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

CEIA ▲ Zona Industriale 54/G, 52041 Viciomaggio – Arezzo (ITALY)
☎ +39 0575 4181 ▲ ✉ info-gsd@ceia-spa.com

www.ceia.net

PREPARE!

COURSES & TRAINING

Preparing Staff Officers for the Fight Against IEDs: CSOC

"Train the minds that will lead the mission". That's the guiding spirit behind the C-IED Staff Officers Course (CSOC), one of the key education programmes of the C-IED COE.

Held twice a year in Hoyo de Manzanares, Madrid, CSOC aims to bridge the gap between national training and the operational-level knowledge required by staff officers and senior assistants deployed in NATO or partner force structures. The course is carefully designed to prepare them to lead, coordinate and advise on the C-IED effort at upper tactical and operational levels.

xInternational Reach and Participation

The February 2025 edition (CSOC 25.1) brought together 21 participants from 10 nations, underscoring the course's strategic relevance and broad international appeal. These officers, representing various services and command levels, immersed themselves in a demanding five-day program combining doctrine, planning, and applied C-IED expertise.

The course was opened by the Director of the C-IED COE, Colonel Javier Corbacho Margallo, who emphasized the importance of investing in intellectual preparation as a multiplier of field effectiveness.

From Theory to Application

The training programme focused on:

- The evolution of the IED threat and countermeasures;
- The integration of C-IED into the NATO Operational Planning Process;
- The role of Human Network Analysis and Attack the Networks (AtN);
- Interagency coordination;
- The development of C-IED annexes and CONOPS;
- And practical planning exercises simulating real-world scenarios.

Students were divided into syndicates to apply their learning through structured planning challenges. The course concluded with a full-scope exercise, validating their knowledge in crafting a C-IED strategy aligned with joint force objectives. The feedback score? A solid 4.6/5, reflecting participant satisfaction and the value of the experience.

Insights and Lessons Learned

Despite high completion rates and strong feedback, the COE identified one area for improvement: entry-level preparedness. Many students came from tactical backgrounds and lacked previous exposure to operational-level planning, a challenge that impacted their ability to contribute evenly across modules.

To mitigate this, the COE will act in these points:

- Enhancing pre-course preparation;
- Stricter selection of participants;
- And exploring modular e-learning content for foundational C-IED awareness.

Building Strategic Capacity

Beyond the classroom, CSOC offers a powerful secondary benefit: network-building. Officers not only gain insight from top C-IED SMEs but also connect with peers from Allied and Partner Nations, fostering interoperability and cross-national cooperation.

“CSOC remains one of our most effective tools to professionalize the C-IED function at staff level. The diversity of backgrounds and the operational focus of the course create an ideal environment to build both knowledge and strategic relationships.”
— MAJ Peter van Achterberg, Course Director, CSOC

Next Courses

The next iteration, CSOC 25.2, will take place 23–27 June 2025 at the C-IED COE in Madrid. For more information and registration procedures, visit www.ciedcoe.org.

DOMEX Course

From Seized Devices to Strategic Intel: DOMEX as a Force Multiplier in Modern Conflict Zones

Coalition forces raided a remote village believed to be a haven for a Violent Extremist Organization (VEO). Among the weapons caches and encrypted radios, operators recovered several smartphones, memory cards, and a ruggedized laptop. At first glance, these devices seemed routine. But within days, the data extracted through Document and Media Exploitation (DOMEX) techniques exposed far more: detailed plans for COTS drone attacks on a UN convoy, procurement lists for Improvised Explosive Device (IED) components sourced from black-market vendors, and encrypted communications linking the group to a known Private Military Company (PMC) operating covertly in a neighbouring country.

This is the power of DOMEX-turning seized digital material into operational and strategic intelligence that can inform targeting decisions, disrupt threat networks, and support legal processes. In today's asymmetric battlespace, where adversaries mix irregular tactics with sophisticated technology, DOMEX has become a force multiplier, enabling armed forces and intelligence units to stay ahead of adaptive enemies.

Benefits That Go Beyond the Tactical

DOMEX is the systematic extraction, translation, processing, and analysis of captured documents and media-both physical and digital. In modern operations, DOMEX has become an outstanding capability, offering critical insights that support decision-making, targeting, and long-term operational/strategic planning.

1. **Providing actionable intelligenc**e: DOMEX enables quick triage and exploitation of recovered/captured materials, allowing commanders and analysts to use fresh intelligence before adversaries can adapt.

2. **Network identification and disruption (Attack the Networks)**: Exploiting contact lists, communications, financial records and media files, DOMEX is able to uncover 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.

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

4. **Force protection**: DOMEX can contribute to preventing attacks through early warning of enemy plans and bring new enemy equipment and Tactics, Techniques and Procedures (TTPs) to light.

DOMEX has proven especially effective in uncovering hybrid threats, where state-backed PMCs and non-state VEOs collaborate in grey-zone operations. In these environments, the exploitation of captured media provides unique windows into adversarial intent that may not be accessible through traditional Intelligence, Surveillance, and Reconnaissance (ISR).

DOMEX in the Modern Battlefield

Modern conflict zones are populated with documents and digital media. Every phone, tablet, drone controller, or USB stick may hold vital clues about enemy intentions, logistics, or external support. DOMEX final step enables the dissemination of those data acquired and analysed, often in time to support real-time operational decisions.

For example, DOMEX has helped uncover how VEOs are adapting commercial drones for reconnaissance and weapon delivery, or how PMCs use messaging apps to coordinate with local militias. Beyond tactical insights, this information feeds into larger intelligence cycles—supporting strategic targeting, counterterrorism, and non-kinetic disruption efforts.

Training the Force: A New DOMEX Training at the C-IED COE

Recognizing the important role of DOMEX in current operations, the C-IED COE has been training NATO personnel in the DOMEX arena, 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.

The primary aim of the DOMEX training is to provide essential technical exploitation skills focused on four main areas, by using specific digital forensic tools, techniques and procedures:

- Document Exploitation **(DOCEX)**: Analysis of data and information acquired from physical substrates and documents.

- Media Exploitation **(MEDEX)**: Analysis of data and metadata from digital media, such as storage devices and laptops.

- Cellular Phone Exploitation **(CELLEX)**: Analysis of all information (current and deleted/ data and metadata) acquired from mobile phones.

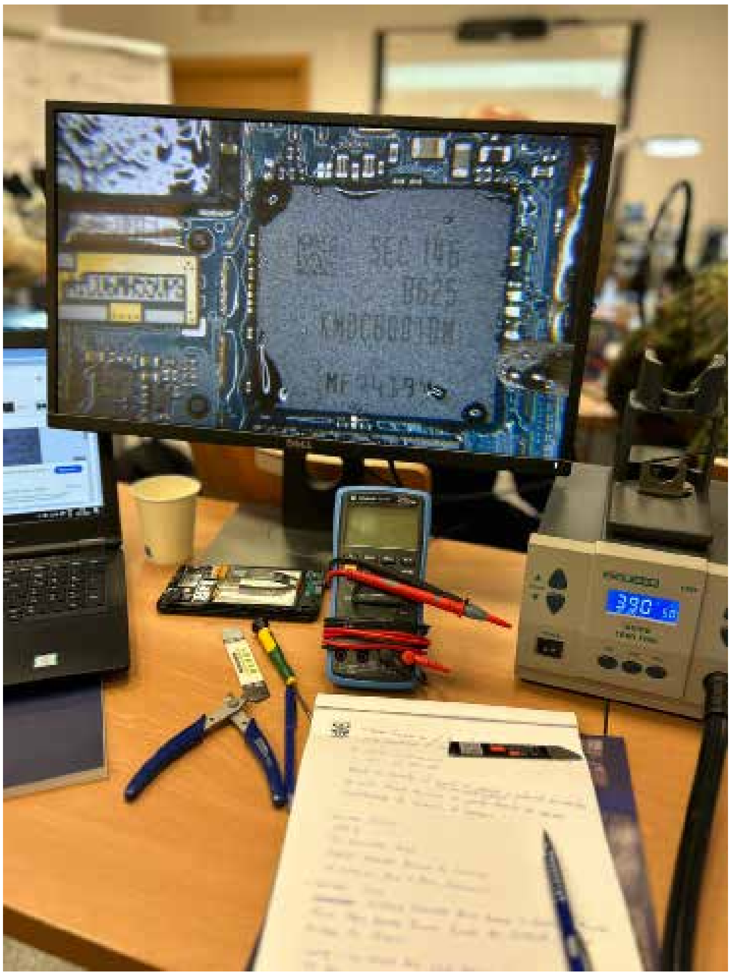
- Unmanned Systems **(UXS)** Exploitation: Analysis of data and metadata obtained from different types of unmanned systems.

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.

After five years, DOMEX will be updated to cover those emerging challenges by creating a new DOMEX training programme comprised by two independent phases, focused on specific personnel needs:

- **Operator Phase (2 weeks)**: Focused on tactical collection, secure handling of digital media, chain of custody procedures and field exploitation skills (including the acquisition of data). This phase certifies operators to process seized devices rapidly and effectively under operational conditions, following evidentiary standards.
- **Analyst Phase (1 week)**: Tailored for intelligence analysts, this module trains participants in interpreting DOMEX outputs by using specifics digital forensic tools, correlating them with other sources, and producing intelligence that supports decision-making at multiple levels.

This new structure ensures a correct flow from field collection to analysis. By separating the roles and focusing on the specific training topics, it maximizes both the speed and depth of exploitation-ensuring that nothing is missed, and everything is actionable.



Conclusion

In modern operations, victory is not only measured by what is captured on the battlefield, but by what is extracted from it. DOMEX turns inert materials into operational and strategic advantage. As adversaries become more flexible and technologically educated, the ability to exploit and analyze seized media becomes essential. DOMEX is a silent force multiplier that operates behind the scenes although, when used, it directly influences the outcome of every mission. The C-IED COE's training initiative ensures that the next generation of DOMEX operators and analysts are skilled not just to collect information—but to turn it into intelligence that saves lives and shapes missions.

ADDING C-IED PERSPECTIVE

CONFERENCES, SEMINARS AND WORKING GROUPS

Connecting Capabilities: C-IED COE at the Military Strategic Partnership Conference 2025

The C-IED COE participated in the **Military Strategic Partnership Conference (MSPC) 2025**, held from 22 to 26 April in **Doha, Qatar**. This annual NATO forum served as a platform to foster strategic ties, to enhance cooperation with partner nations, and to identify new avenues for Defence Capacity Building (DCB), a mission that aligns directly with the Centre's commitment to supporting global efforts in countering the IED threat.

A Platform to Strengthen Global Ties

The MSPC brought together NATO HQ representatives, Training and Education Facilities (including COEs), and partner nation delegations. It featured three main elements:

- Plenary Sessions, focused on policy and institutional updates;

- A Marketplace, allowing institutions to showcase their expertise;

- And most importantly, Bilateral Meetings between NATO stakeholders and partner nations.

While the plenary sessions offered limited interaction, the **marketplace and bilateral meetings** proved essential for relationship-building and future planning.

W**C-IED COE's Presence: Visibility and Engagement**

Representing the Centre was OF-4 **Fernando Martel**, who actively engaged with stakeholders and participated in bilateral meetings with **Tunisia**, **Kazakhstan**, and **Jordan**-all nations where C-IED programmes are planned or ongoing. Although the conference format posed logistical challenges (requiring pre-arranged access to limited-capacity meetings), these interactions reaffirmed the C-IED COE's relevance and growing reputation among partner countries.

The **marketplace booth** also served as a valuable engagement tool, particularly for delegations already familiar with the C-IED COE's capabilities. This underscored the need to enhance the Centre's public presence through improved visual materials, promotional videos and targeted content.

Laying Foundations for Capability Building

Participation in MSPC aligns directly with NATO's strategic goal of **building partner capacity**. It allows the C-IED COE to:

- Track DCB efforts already underway in regions of interest (North Africa, Central Asia, the Gulf);
- Offer tailored education, training and advisory support;
- And strengthen cooperation with institutions, such as the NATO-ICI Regional Centre in Kuwait and relevant Joint Force Commands.

The bilateral discussions opened doors for future collaboration in **WIT, DOMEX, ATNOC** and **Train the Trainer** modules—all of which can significantly elevate local counter-IED competencies.

Attending MSPC allows the C-IED COE to remain visible and relevant across NATO's wide partnership spectrum. It is a strategic tool to connect with countries that seek our expertise, but may lack channels to request it directly.

JOIN UP! BE PART
TO FIGHT IE

OF THE C-IED COE ED SYSTEMS

YOU CAN BE PART OF OUR EVENTS AND COURSES VISIT: ciedcoe.org

KANGAL
aselsan
DRONE MINI/MICRO UAV
JAMMING SYSTEM
KANGAL™ protects critical facilities, military zones, strategically significant urban and rural areas from Mini/Micro UAVs and FPV threats.
aselsan 50 years

UPCOMING EVENTS 2025

C-IED COE courses second semester 2025

This is the C-IED COE planning for 2025 with regard to courses approved by the Steering Committee on 14 November 2024. Below dates may change due to unforeseen reasons. No rights can be inferred according to this schedule.

NATO Weapons Intelligence Team Course (WIT) 25.2
2-Sep
Hungarian Defence Forces NCO Academy (Szentendre, HUN)

Analyst Notebook User Course (ANUC) 25.3
29-Sep
C-IED COE (Madrid, ESP)

C-IED STAFF OFFICER COURSE (CSOC) 25.3
20-Oct
C-IED COE (Madrid, ESP)

DOMEX Train the Trainers 25
Sept/Oct TBD
C-IED COE (Madrid, ESP)

DOMEX- AtN Operator
27-Oct
C-IED COE (Madrid, ESP)

DOMEX -AtN Analyst
10-Nov
C-IED COE (Madrid, ESP)

AtN Operational Course (ATNOC) 25.2
17-Nov
C-IED COE (Madrid, ESP)

NATO Weapons Intelligence Team TDC Course (WIT)
1-Dec
C-IED COE (Madrid, ESP)

CIEDAC25: C-IED COE Launches a New Flagship Event

The C-IED COE is proud to announce the launch of its Annual Conference-CIEDAC25, which will take place in Málaga, Spain, from 9 to 12 June 2025. This newly established event replaces the former Technology Workshop (TECHWS) and Interagency Workshop (IAWS), combining their strengths into a single, strategic platform designed to unite the global C-IED community.

With the theme “Countering the IED System in Support of Multi-Domain Operations”, CIEDAC25 aims to create a collaborative environment for sharing knowledge, operational experiences, innovation and solutions among military forces, law enforcement agencies, international organizations, academia and industry.

Main Focus Areas

The conference will address:

- Evolving threat dynamics and IED trends.
- Technical Exploitation techniques and practices.
- Emerging disruptive technologies supporting C-IED.
- C-IED education and training initiatives.
- Operational observations and lessons identified.
- Integration of C-IED efforts into the NATO Warfare Development Agenda (WDA).

A Space for Dialogue and Innovation

CIEDAC25 will feature keynote presentations, expert panels, interactive roundtables and industry exhibitions, fostering meaningful exchanges across domains and disciplines. The programme also includes social and cultural activities to strengthen informal networking and community ties.

Hosted at the ILUNION Hotel Málaga, the venue will offer the professional setting and logistic accessibility needed to accommodate a diverse audience of practitioners and decision-makers.

By consolidating its major events into this single annual conference, the C-IED COE underscores its role as a central hub for the C-IED community of interest, committed to addressing emerging challenges and enhancing multinational cooperation.

We look forward to welcoming the community to CIEDAC25 in Málaga—a new milestone in our collective fight against the IED threat.

Precision Moves. Tactical Tools

IDEALBLASTING.COM

SPOT deploys with the
RDAS (Remote Disrupter Aiming System) — delivering
real-time threat data on a mission-critical platform.
Whether it's robotic payloads, disruptors, or EOD support kits,
Ideal Blasting equips you for the next move.
This is just one piece of the mission.

Soldier in the Spotlight

Lt. Col. Rui Cordeiro (PRT A), DtD Branch

Let's start from the beginning. What was your path into the military? What inspired you to choose a career in the Portuguese Army?

It feels like it was just yesterday, but actually it's been a few years... thirty-one to be exact! When I finished high school, military life was one of the options I was considering, along with going to university to continue my studies in Computer Engineering. When the opportunity to join the Portuguese Army as a volunteer came up - which was something that fascinated me for the adventure and the possibility of serving my country - I didn't think twice when I was called. After joining the military, in 1997, I applied to the Military Academy and ended up continuing my studies in Military Engineering.

It turned out to be the best choice I could make, as the Engineering Branch, due to its diversity of employment options, ended by sparking my interest in Sappers, EOD and C-IED activities, besides the fact that it allowed me to address other important MILENG areas like Military Bridging or Constructions.

Could you tell us about your academic background and how it has complemented your military career?

As an engineering officer my training was diverse and comprehensive, but I would highlight three fundamental stages that supported my military career. The first, resulting from my academic background with a Degree in Civil and Military Engineering (Chartered Civil Engineer), having subsequently specialized through specific training in Explosives, Demolitions and Minefields (at the national Engineers School), the Explosive Ordnance Disposal for Officers Course (here in Spain), and right after, the Counter-IED Course (also at the national Engineers School).

The second stage would start after I obtained my Advanced Staff College Qualification (Postgraduate qualification in Military Sciences – Security and Defence), which allowed me to perform functions in the Army General Staff for five years, essentially related to strategic planning and military capabilities development, but also to innovation, in coordination with EU and NATO bodies.

And third, more recently, at the performance of my duties here at the C-IED COE, where I attended the NATO C-IED Staff Officers Course and the NATO WIT Course, which allowed me to optimize and deepen my knowledge and to develop my activity as Director of the NATO WIT courses.

Was your early military experience already connected to the field of Explosive Ordnance Disposal or C-IED, or did that come later?

Yes, in some way, because in the Portuguese Army, EOD, WIT and C-IED capabilities are mostly tied to Engineering. For that reason, I was one of the members of the initial Working Group that was responsible for developing the Portuguese Army's C-IED doctrine. Of course, as time went by, I ended up adapting some concepts related to C-IED and its enablers (like WIT, EOD and Route Clearance), due to the roles I held throughout my career, whether that was in the training and operational structure, or even in my latest years in the Army Staff.

How did you first become involved in the Counter-IED field? Was there a specific mission or role that shaped that interest?

The interest and specialization in Counter-IED arose naturally during my training as an EOD officer, but also through its inclusion in national doctrine. When I was Head of the Explosives and Countermeasures Training Centre and Assistant Officer at the C-IED/CBRN Centre of Excellence, I was responsible for the training provided to the Army in areas like Sappers, EOD and C-IED. At that time, I was necessarily involved in education and in the inclusion of Lessons Learned throughout the theaters of operations in which Portugal participated.

Of course, this interest was also "sharpened" when I was deployed in Lebanon (2006/07 and 2011/12), where security concerns and the IED threat were transversal to all forces deployed there.

What were your first impressions when joining the C-IED Centre of Excellence? How did your expectations compare to reality?

Although I had already some information from my predecessors, who had told me how much they had enjoyed working at the COE, I was very eager to work in a multinational environment like the one that we have here. Fortunately, I found a great working environment, where it is really easy to talk and work with everyone. This is the unique character of this Centre. Multinationalism here isn't an obstacle, but a way to bring different perspectives together - which is something that the Iberian people, and especially the Portuguese, really value.

Of course, my adaptation was somehow easier because I already knew Spain, Madrid and the Engineers' Academy, as I was here attending the EOD course at the International Demining Centre 15 years ago. In that sense, the language and cultural barrier that might be a problem to others, was almost non-existent (the truth is that Portugal and Spain have a lot of things in common, and the Spanish culture is in some ways very similar to ours).

Could you describe your current role within the DtD Branch? What are your main responsibilities and areas of focus?

Currently, I am head of the Mitigation Section, whose main focus is identifying and analyzing activities, technologies and TTPs involved in mitigating the effects of IEDs, to enhance the protection of personnel, equipment, operations and infrastructures. This involves evaluating and integrating the most relevant technological features and operational factors across a range of potential C-IED scenarios. By comparing operational mitigation needs with available technological solutions, we can better assess current capabilities and identify gaps or requirements for future development.

In this context, efforts also focus on concept development and experimentation, supporting the establishment of standards for evaluating IED mitigation systems. Collaboration in the analysis of Lessons Learned - drawn from ongoing operations or shared by Allied Nations - plays a crucial role in refining mitigation strategies. This work contributes to the identification of effective TTPs and Technologies, guiding future doctrinal development aimed at reducing human exposure to IED threats.

Additionally, and this is my most challenging role, I'm responsible for the NATO WIT Training (WIT and WIT Training Development Courses) and all WIT related subjects as Subject Matter Expert (SME).

You've directed and participated in various courses at the COE, such as the WIT, the WIT TDC and the CSOC courses. What makes these training activities particularly relevant for today's missions?

The Weapons Intelligence Team (WIT) or Field Exploitation Level 1, is conducted on-site at the tactical level, by a pool of trained specialists that investigate IED-related incidents when tasked. It is the first layer for gathering information that can be used to attack the IED system. It is a non-invasive process and has a minimum manipulation of Collected Exploitable Materials (CEM), ensuring its forensic validity.

WIT Training is an integrated and common effort, not only related to the fight against the IED system, but also contributing to the security of Allied Nations and all troops deployed in operations. From WIT activity and assessment, we can get Tactical & Technical characterization of an IED event, leading to Pattern Analysis, TTPs, Event Signatures and Device Profiling, and this remains highly relevant on current operations.

From your perspective, how has the threat of IEDs evolved in recent years, especially with the integration of new technologies like drones or 3D-printed components?

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, come up with countermeasures, and share intelligence.

In addition, these advancements allow both state and non-state actors to create customized, high-tech devices, increasing the complexity of counter-IED efforts and requiring continuous adaptation and cooperation among Allied forces.

What have been some of the most valuable professional experiences or lessons learned during your time at the COE?

I would say that the most valuable experiences have been the outstanding work environment that I find here at the COE, highly professional and effective and at the same time very informal, what makes everything easy.

Regarding professional experiences, as you can imagine, being Course Director of the WIT courses held in Romania and Hungary allows me to frequently interact with different people from different nationalities, perspectives and experiences, and that makes my job really interesting and fulfilling.

Of course, I cannot forget the opportunity I was given during the visit of HM Felipe VI, King of Spain, where I was one of the chosen SMEs to brief him about the NATO WIT course and other related training activities, including a small demonstration of capabilities. It is something that I will never forget for the pleasure and honour of such a task.

You work in a truly multinational environment at the COE. How has this influenced your approach to interoperability and knowledge sharing?

You can see different viewpoints, cultures and systems in a multinational setting like the one that we have at the C-IED COE. This makes everybody more flexible and inclusive when working on interoperability. It also encourages sharing knowledge openly and adaptively across countries and fields of expertise. Furthermore, it illustrates how important clear communication and standard methods are to overcome differences.

Looking forward, what capabilities or focus areas do you believe should be prioritized by NATO and partner nations in the field of C-IED?

I wouldn't mention a focus or prioritization on specific areas, but rather a reinforcement of the importance of C-IED, as a discipline, and the C-IED Technical Exploitation as a tool to boost the fight against the IED system in NATO operations.

As I usually say, we can see in several conflicts taking place all over the world (and not only in Europe), that IEDs continue to be a weapon of choice, both by non-state and state actors. Accordingly, the fight against the IED system continues to be essential, and ensuring the security of troops deployed in theaters of operations is still a primary objective, by reducing or eliminating the threat posed by the use of IEDs, whatever their type.

Considering its unique capabilities, that can help identify the IED threat, the components used and the sources of supply, as well as linking cases and individuals and contributing to the counter measures effort (both tactical and technical), I think that WIT / C-IED Technical Exploitation Level 1, and also DOMEX as a level 2 activity, are relevant capabilities for any NATO Commander and NATO Operation and should be supported in that sense.

Finally, on a more personal note—what advice would you give to young officers considering a specialization in C-IED or Technical Exploitation?

Above all, and contrary to what many may tell you, the IED threat is still very relevant (conflicts in the East and Middle East are a living proof of that), even though the most "traditional" vectors have been pushed into the background compared to the current preferred ones - unmanned systems and FPVs.

Focusing my answer on my area of expertise, I would say that from the Defeat the Device perspective, without forgetting what we have learned over the years, we must keep learning and adapting to new technologies and how they can be used, not just by the opponent but also by Allied forces, to effectively Protect and Mitigate the effects of a possible IED.

Technical Exploitation shows up as one of the main tools at the tactical level to support Intel and targeting cycle, with the goal of Attacking the Networks. From what I understand, it is one of the most attractive and relevant areas in the fight against the IED system, which is also constantly adapting to new threats. That's why I think it will be rewarding to invest in personal specialization in these matters.

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.
- 🌍 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

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