YOU ARE IN THE C-IED

CHESSBOARD

INSIGHTS FROM NATO's C-IED EXPERTS

DEC 2024 | ISSUE 02

H.M. the King of Spain Visits the C-IED 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
LTC José Manuel Rufas Simón (ESP A)
LTC Fernando Martel Muñoz-Cobo (ESP A)
LTC Rui Cordeiro (PRT A)
LTC Félix Ortega Medina (ESP A)
LtCdr. Murat Aydogmus (TÜR N)
Capt. Manuel Pinillos Mitge (ESP A)
Capt. Enrique Sevillano (ESP A)

DISCLAIMER

CONTENTS

Counter-Improvised Explosive Devices Centre of Excellence

NATO Accredited Centre of Excellence

CTRA. M-618 COLMENAR VIEJO-TORRELODONES KM. 14
28240 HOYO DE MANZANARES, MADRID-SPAIN
+34 91 856 10 48
INFO@CIEDCOE.ORG
WWW.CIEDCOE.ORG

NEWS FROM OUR WATCH

C-IED COE
Director's Letter

As the Director of the C-IED COE, I am pleased to introduce to you a new issue of our magazine, in which we have put all our effort to be of help to the C-IED Community of Interest (CoI).

First, I would like to express my gratitude for the **visit of HM Felipe VI, King of Spain**. Ten years after his first visit as Prince of Asturias, it has been a huge honor to receive HM as the King and to have the opportunity to show the evolution of the Centre and the current challenges we face to help fight the IED threat, working at the left of the boom.

Besides, I would like to mention 2 major events organized by the Centre for the benefit of the C-IED CoI: the **6th C-IED Technology Workshop**, held in Seville last May, and the **Lessons Learned Workshop (LLWS24)** held in Madrid last June.

Regarding future events, I am pleased to announce that the COE will take advantage of the experience acquired in the last decade to organize the **C-IED Annual Conference 2025 (CIEDAC25)** in Málaga. It will be a **multi-disciplinary** event that will gather C-IED technology, inter-agency collaboration and lessons learned. I am sure it will attract the interest of the C-IED related agencies, bodies and organizations and will be the venue to foster information sharing, project development and fruitful debate about the future trends in the field.

Starting with this issue, our intention is to go beyond the mere publication of information regarding the Centre's events and activities, so we have started including articles aimed at spreading knowledge in the C-IED realm. A significant part of this issue is **focused on the C-IED situation in the African continent**. Likewise, we have included articles on various projects led by the Centre and another on C-IED in support to NATO Cognitive Warfare Initiative.

I would like to end this letter by reaffirming our intention that this magazine consolidates as proof of the continuous work developed by this Centre during the past 15 years for the benefit of the C-IED Community of Interest. We will persist in the effort to be on the front line in our discipline, to improve our way of communicating it and to contribute to achieving the interests of our Sponsor Nations, the Alliance and the whole international community in the fight against the threat posed by the use of IEDs.

COLONEL JAVIER CORBACHO MARGALLO (ESP A)
IS THE C-IED COE DIRECTOR

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)

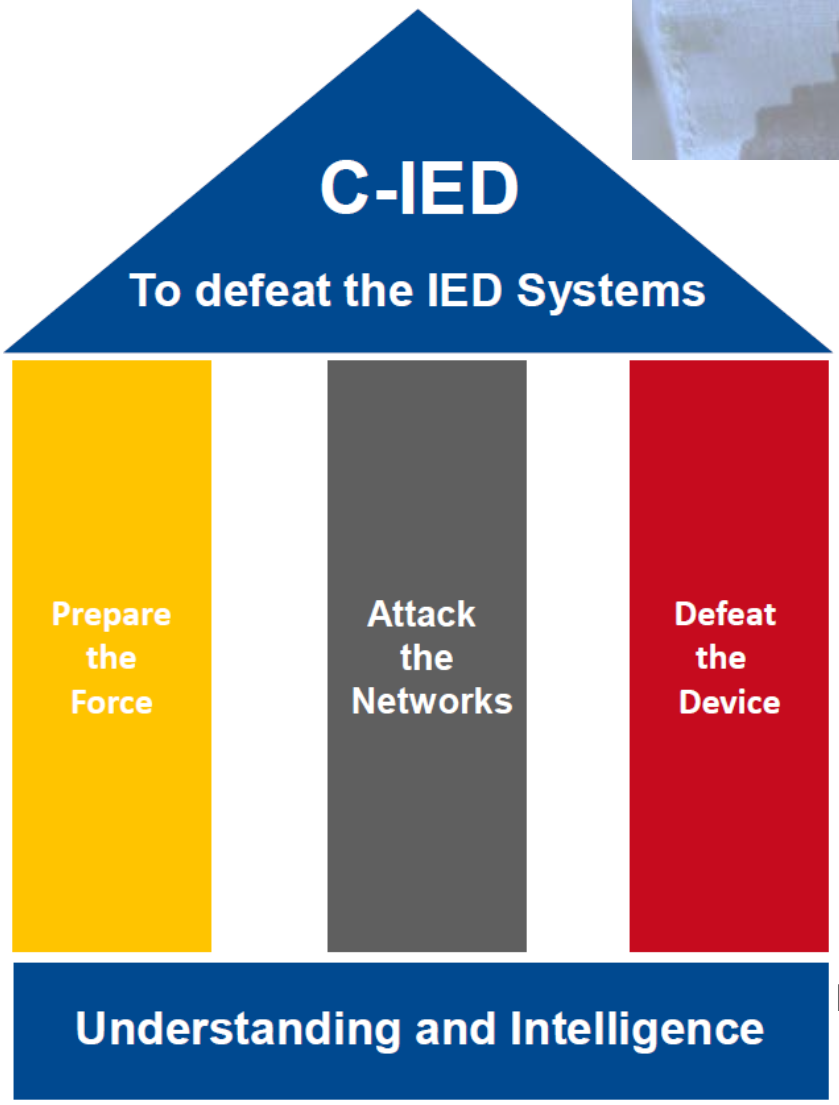
MORE INFO
act.nato.int/about/centres-of-excellence

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.

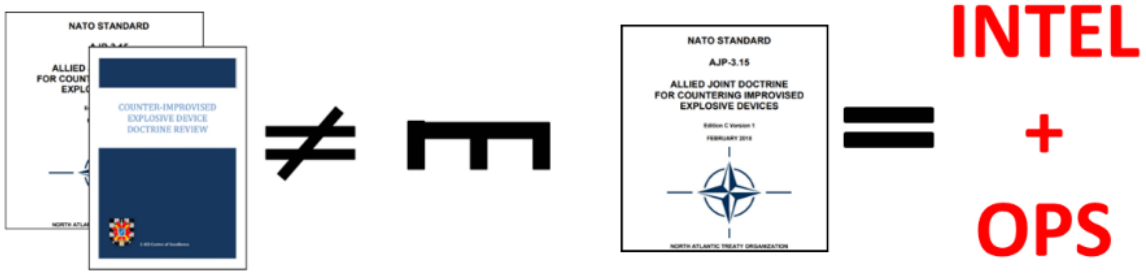
The C-IED COE is a proud member of the COE community

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



H.M. the King of Spain

C-IED COE HIGHLIGHTS

H.M. Felipe VI visits the C-IED COE Hoyo de Manzanares

His Majesty the King has visited the Counter-Improvised Explosive Devices Centre of Excellence (C-IED COE), which provides expertise and leadership in combating improvised explosive devices to enhance the security of Spanish and allied forces deployed in operations. It is one of the 30 'NATO Accredited Centres of Excellence,' located in the town of Hoyo de Manzanares, Madrid. Its accreditation as a COE meets the quality standards required and certified by NATO's Allied Command Transformation to be considered a 'NATO Education and Training Facility.'

Upon his arrival at the C-IED COE, His Majesty the King was accompanied by the Chief of the Defense Staff, Admiral General (ESP N)Teodoro Esteban López Calderón; the director of the Engineers Academy, Col. (ESP A)Juan Pedro Moral Albadalejo, and the director of the C-IED COE, Col. (ESP A)Javier Corbacho Margallo; he was honored by a guard.

This is H.M.'s second visit to the Centre, the first as King of Spain.

Next, King Felipe proceeded to the Conference Room where a presentation on the Centre and its work took place. Among its missions, the COE supports NATO, NATO partners and the International Community through the development and delivery of various trainings and specialization courses in combating Improvised Explosive Device Systems, thus contributing to the increased security of deployed troops by reducing or elimi-

nating the threat of improvised explosive devices, particularly those from terrorist networks and insurgents.

Following His Majesty the King's signing in the Book of Honor and a group photograph with the staff stationed at the C-IED COE, King Felipe witnessed various demonstrations from the Weapons Intelligence Team (WIT) course, presented by the Chief of the Branch 'Defeat the Device', Colonel (TUR Army) Umut Çetin, and the course director, Lieutenant Colonel (POR Army) Rui Cordeiro. Then, the Chief of the Branch 'Attack the Networks', Lieutenant Colonel José Manuel Rufas, presented the work performed in his Branch, followed by a demonstration in the IED Lab, Digital 3D-Modelling of IED & IED Components in support to C-IED Training R&D (Research & Development) Project, presented by Colonel Umut Çetin, Master Sergeant David Herraiz and Captain Manuel Pinillos.

Lastly, he attended an explanation about the Document and Media Exploitation Course (DOMEX), presented by the course director, Major Juan Manuel Mancilla and Master Sergeant Jesús González Sanz.

Spain plays an active role in the Defense Against Terrorism Work Programme within the framework of the North Atlantic Treaty Organization, leading the 'Counter-Improvised Explosive Devices' Initiative. For this purpose, a specialized centre on the described threat was established within the Ministry of Defense and in cooperation with other countries and organizations, configured to obtain the consideration of 'Centre of Excellence' issued by NATO, thus becoming an international reference in the fight against improvised explosive devices.

The C-IED COE was offered by Spain to NATO as part of its network of centres of excellence and accredited by the Alliance in November 2010. For the development of its purposes, it involves the participation of Allied nations and the support of our Armed Forces, Civil Guard, National Police Corps, National Intelligence Centre, and other international organizations, particularly the European Union.


IMPROVISED EXPLOSIVE DEVICES
CENTRE OF EXCELLENCE

NATO OTAN

Accredited COE

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

MORE AT: nato.int

ENGAGE!

EVENTS

6th Technology Workshop

The 6th C-IED Technology Workshop was organized by the C-IED COE and held at Hotel Meliá Sevilla from 28 to 30 May 2024. The aim of this biennial workshop was to provide the C-IED Community of Interest with an in-depth overview of the latest operational gaps/requirements based on the current conflicts and the emerging and disruptive technologies in both international and national projects.

The event serves as an ideal environment for defining end-user requirements, as well as for exchanging information and gaining knowledge about the tools being developed to address the evolving threat of IEDs and technical exploitation.

This workshop was focused on the following topics: Overview of IED Threat and Latest Operational Gaps and Requirements, Organizational Initiatives in C-IED Research and Development, National Presentations on Specific C-IED Technologies Activities and R&D Projects, Technologies Supporting C-IED Training, Technical Exploitation for Operational Needs, Advanced Standoff Detection and Neutralization Technologies, Future C-UAS (Countering Unmanned Aircraft System) Solutions for Explosive-Laden Threats, Future USV/UUV Solutions for Countering IED in Maritime Domain and IED Threat Mitigation-Current and Emerging Technologies.

C-IED TECH triumphs over threats

The 6th C-IED Technology Workshop 2024 (TWS24) brought together over 190 delegates from various national and international organizations, Ministries of Defense (MoDs), law enforcement institutions, research centres, industry and academia.


MELIÁ
SEVILLA


6TH C-IED
TECHNOLOGY
WORKSHOP


INERT PRODUCTS

The Technical Exploitation in Water Environment Trials Seminar

TEWE24

The "Technical Exploitation in Water Environment 2024 (TEWE24)" Trials Seminar was held in Hoyo de Manzanares (Spain) from 19 to 21 November, organized by the C-IED COE and sponsored by NATO.

This Seminar was a practical continuation of the outputs from previous editions of the TEWE (2021, 2022 and 2023) along with those from the Alternate Threat Scenarios (ATS) Seminars (2022 and 2023). This event is funded by Voluntary National Contribution Funds (VNCF) through the intermediation of NATO HQ International Staff Emerging Security Challenges Division (ESCD).

The generic objective of the event was to put experts (scientists, specialists and technicians) related to Technical Exploitation (TE) in water environment (open, inner, confined, swallow, subterranean, residual and artificial waters) and supportive disciplines together.

The event created a favorable space to enrich the experts' technical skills with scientific knowledge, to share experiences, to promote best practices and to improve collaboration among agencies and security forces.

During the Seminar, several experts presented the results of the trials carried out by diverse forces and agencies about the following topics:
Trial series 1 – Design, manufacture, tests and final technical exploitation of explosive-laden unmanned aircraft systems (UAS).

Trial series 2 - Design, manufacture, tests and final technical exploitation of explosive-laden unmanned surface vehicles (USV).

Trial series 3 – Design, manufacture, tests and technical exploitation of underwater gas-based improvised explosive devices.

Trial series 4 – Study on current methods for revealing latent fingerprints and analysis on the most recommendable methods for collected exploitable material as taken from high-humidity environments.

Based on all presentations and discussions, several specific conclusions were drawn:

- Collaboration, knowledge-sharing and practical applications across multiple domains are essential.

- Explosive-laden unmanned vehicles represent a growing (and hard to defeat) threat due to their adaptability, cost-effectiveness and resistance to countermeasures, along with the proliferation of related tactics and technologies.

- There is an identified gap in capabilities for explosive-laden unmanned vehicles' technical exploitation.

- Incorporating TE into NATO exercises and aligning doctrine revision is essential for staying ahead of evolving threats.

- The main question is if the current NATO technical exploitation capabilities are sufficient to assure the provision of adequate TE capabilities in water environment to Allied operations.

- Most of the actors/bodies (e.g. law enforcement, firefighters, intelligence services...) participating as audience in Alternate Threat Scenarios Seminars' initiative are also unilaterally conducting realistic trials as derived from former ATS seminars. This poses a clear evidence of the relevance, acceptance and resulting benefits from the ATS initiative led by the C-IED COE.

CHESSBOARD FOCUS:

In this issue we launch a new section focusing on relevant issues

2024 Threat Dynamics in Sahel & West Africa

During 2024, due to the scenario of failed states, both Jama'at Nusrat al Islam wa al Muslimeen (JNIM) and Daesh Sahel Province (ISSP) are not only quickly expanding in the Sahel region, but also strengthening their capabilities. Meanwhile, Daesh in West Africa Province (ISWAP) is gaining ground and consolidating the support from the Nigerian population.

The influence activities of JNIM are directly managed through "az-Zallaqa Media" (JNIM), while ISWAP and ISSP are supported by the main Daesh's media offices (e.g. "Hallumu", "Amaq", Islamic State News" ...).

Figure 1 – Latest propaganda on JNIM's last actions 05SEP-04OCT2024 (Source: RocketChat)

The increase in JNIM activities against border posts in Western Mali creates opportunities for self-sustainment, while the operations in Southern Mali are degrading the lines of communication. The attacks over the capital, Bamako, are also significatively increasing.

The security situation in Burkina-Faso is not evolving much better and it is negatively affecting the regional trade. Although they have had a relative success in Kidal, the campaigns by Malian forces and Russian auxiliaries in Northern Mali have not achieved the expected results in degrading JNIM. On the contrary, JNIM is gaining rural support around Eastern and Northern Burkina-Faso, and this allows them to besiege government-held population centres.

The alliance between JNIM and the Permanent Strategic Framework for the Defense of the People of Azawad (CSP-DPA, whose official name was changed by "Azawad Liberation Front" FLA on 28 November 2024) has dramatically affected the capabilities of the Malian forces and their Russian partners.

Daesh in the Sahel Province established its dominance over JNIM in the Tri-border Area (Liptako-Gourma), where they have been occasionally clashing: ISSP is showing signs of consolidating its control in Northeastern Niger (e.g. growing zakat extorsion and moral control) and in Southwestern Niger.

There are indicators about the transition of ISSP from mass violence to territorial control and governance. But on the other hand, they are suffering from internal factionalism and tensions between different commanders.

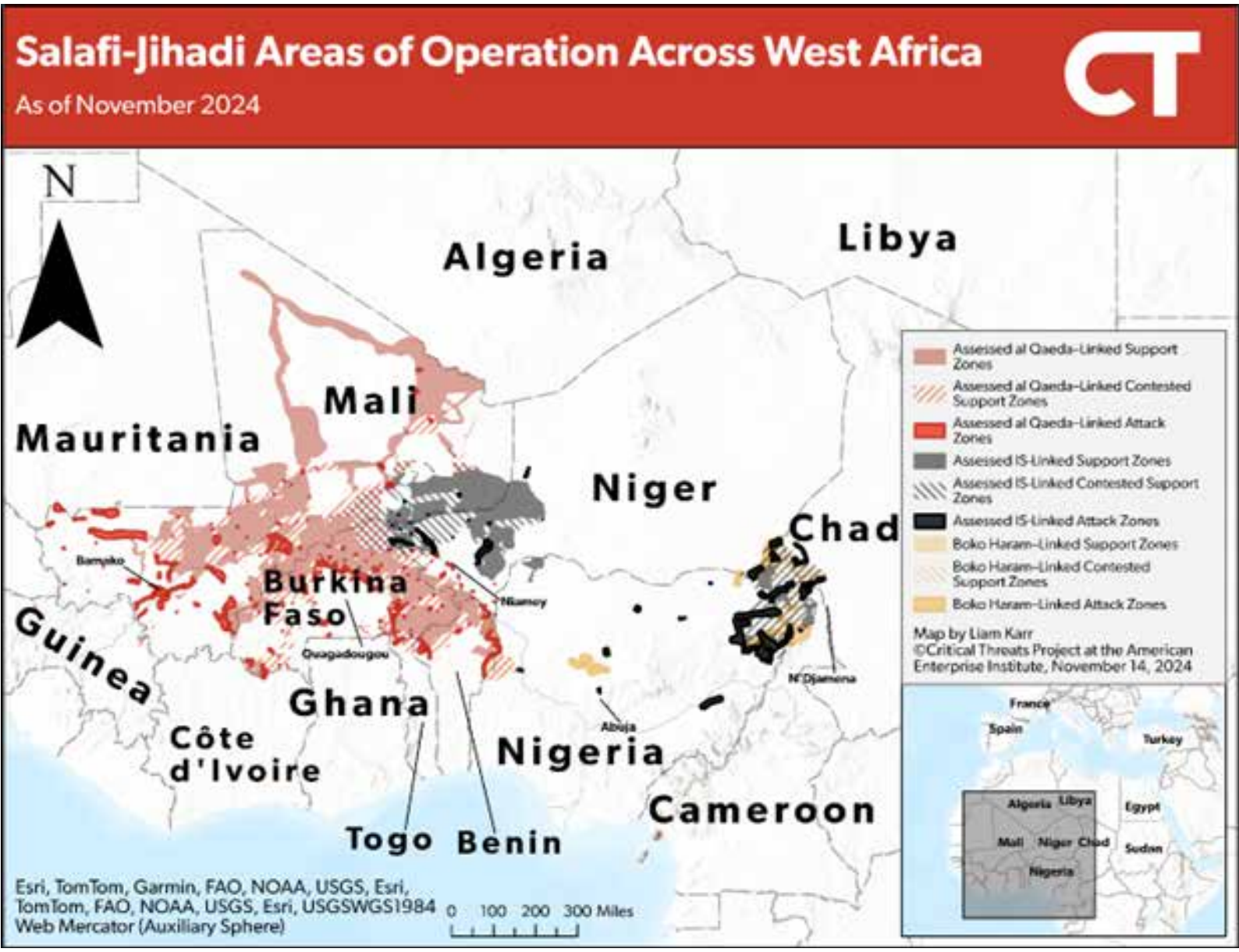


Figure 2 – Map of adversary human networks in Sahel and West Africa areas (Source: www.criticalthreats.org)

The Daesh-linked Lakurawa faction has increasingly infiltrated Northwestern Nigeria's Kebbi and Sokoto states from neighboring Niger and Mali, while other groups linked with JNIM have also been crossing from Benin to Nigeria.

The threat of JNIM and ISWAP moving towards the Northern borders of the coastal West Africa states of Cote d'Ivoire, Ghana, Togo and Benin is still alive. Previous attacks have been reported inside Benin and Togo (a JNIM one on 2 October 2024), while Ghana and Senegal are currently suffering from a relative economic and political instability which could make them more vulnerable to violent activities. Simultaneously, there is a growing migration from the Sahelian area to coastal West Africa states (over 110,000 people in October 2024, according to the UN Refugee Agency Regional Bureau for West and Central Africa UNHCR RBWCA).

It is relevant to point out the dramatic decrease in the fights between JNIM and Daesh franchises, not only in the Sahel region, but also in West Africa. It seems that potential rear support zones in Benin, Niger and Northwestern Nigeria could be helping facilitate and coordinate activities and resources between JINM and Daesh affiliates, as well as expand actions to the coast.

Last October, the number of attacks in Chad and Cameroon increased: it could be due to the confluence of the operations against local military forces, the fights between ISAWP and the former Boko Haram's faction Jama'at Ahl al Sunna li Da'wa wal Jihad (JASDJ) in Lake Chad area, and the ethnically based violence in Nigeria.

Meanwhile, ISWAP is strengthening their territorial control and governance in Northern Nigeria, all through a structure based on Wilaya (provinces) and their respective Mantika (districts).

Although the Russian Private Military Companies (PMCs) replaced Western presence inside Africa under a pretended aim of defeating terrorism, the violent extremist organizations have seen their territorial influence grow along with making governmental forces remain near big cities.

With regards to Tactics, Techniques and Procedures, the most remarkable trends in 2024 are based on the increase in the use of vehicle-borne IEDs (also in their up-armored version in Nigeria), along with the initial steps in the utilization of explosive-laden drones (JNIM, CSP-DPA/FLA).

Figure 3 – Poster on Daesh operations 14-20NOV2024, including 12 attacks by ISWAP (Source: RocketChat)

References:
C-IED COE internal database
www.observatorioterrorismo.com
www.thesoufancenter.org
www.criticalthreats.org
www.understandingwar.org
www.acleddata.com
RocketChat

Partnering for Progress: NATO's Role in Africa's C-IED Evolution

In recent months, the C-IED COE has had the opportunity to attend several forums and events in Africa related to countering improvised explosive devices (C-IED). These ranged from regional forums, such as the Global Counter-Terrorism Forum West Africa Working Group (GCTF WAWG), to continent-wide conferences like the annual Africa C-IED Conference, as well as national initiatives like the Tunisian TC2E (Tunisian C-IED Centre of Excellence) and UN (United Nations) working meetings held at the Regional Service Centre in Entebbe, Uganda.

These activities demonstrate, on one hand, that the continent and the organizations operating there recognize that their current approaches to fighting IEDs are either ineffective or falling short. On the other hand, they also highlight NATO's awareness of the issue in Africa and its willingness to assist organizations and nations in developing proper C-IED doctrine and training.

From these events, several key observations can be drawn. While Africa is by no means a homogeneous continent, with its diverse political systems, military structures, and varying levels of economic development, the threat posed by IEDs is relatively consistent. As a result, the lessons learned can likely be applied across the region, as most countries and organizations are at a similar stage of evolution in their C-IED capabilities, with some exceptions.

Generally speaking, African countries fall into two categories: those without any C-IED training programmes and those that have made serious

Current approaches fighting IEDs in Africa are falling short

efforts to develop them. However, even the latter often focus exclusively on tactical, device-centric, and operator-centred training. This traditional approach to IEDs is a method NATO itself found insufficient several years ago. African nations are now becoming increasingly aware of these limitations, especially as IEDs are used more extensively.

While many countries and regional organizations are eager to advance beyond this stage, they face challenges in finding partners or organizations to guide them. Numerous private enterprises and national initiatives offer training and equipment, but much of it remains device-focused. This is where NATO can step in, providing advice and assistance in developing broader capabilities to address the systems and networks behind IED threats, rather than solely focusing on the devices themselves.

Achieving this, however, is no simple task. What steps can NATO take to help improve C-IED capabilities on the continent?

1. Active Engagement in Events:
NATO should continue participating in the aforementioned forums, taking on a more active role. These events provide an excellent platform for spreading key concepts about what effective C-IED strategies entail. For example, the distinction between defensive and reactive approaches versus proactive and offensive measures is critical. Additionally, the focus should extend beyond training operators and units to preparing staff officers in headquarters roles, particularly in operations and intelligence. Notably, even some NATO nations struggle to fully grasp these points.

2. Developing Training Programmes and Doctrine:
Beyond initial device-centric training, NATO could assist in developing technical exploitation capabilities and programmes like Weapon Intelligence Teams (WITs). These capabilities would enable African nations to analyze and understand devices and their underlying systems. Such advancements would not only bolster defensive measures, but also lay the groundwork for offensive capabilities.

3. Training Key Leaders and Staff Officers:
Perhaps the most challenging yet impactful step would be assisting in the training of key leaders and staff officers. This would enable them to "close the circle" by moving from defensive measures to network disruption strategies.

In pursuing these objectives, it is essential to recognize that NATO's doctrine cannot be directly applied to individual nations or to the UN. However, NATO's philosophy and foundational concepts—such as the operational level, interagency cooperation, and joint operations—can be adapted to support the development of tailored doctrines and strategies. These concepts may need significant adjustments for single nations with different structures.

In summary, Africa faces a significant IED problem across many of its regions. While political complexities cannot be ignored, NATO has been supporting various countries and organizations, albeit with a focus on equipment and tactical, device-centric training. While these efforts are important, it is time to go further, helping African nations adopt offensive measures to combat IED threats. Realistically, training and concept development alone will not eliminate the IED threat in Africa, but they can certainly help mitigate its impact and save lives.

C-IED Observations & Lessons Identified from Sahel & West Africa

Years of conflict in Sahel (Mali, Burkina-Faso, Niger...) and West Africa (Nigeria, Chad, Cameroon, Benin, Togo...) have allowed the study of their dynamics, both as based on direct reports or just through an indirect watch over them.

The last events in Sahel and West Africa show a lack of effectiveness in Counterterrorism operations by African nations, African multinational forces, United Nations missions, and even Western operations. In fact, Western nations have been forced to leave missions like Sabre, EUTM-Mali, Barkhane, MINUSMA, Takuba... One key reason behind the failure of Western operations is the highly effective Russian influence campaign in Africa, which has exploited the resentment against France by the population of their former colonies.

The potential lessons identified after analyzing those facts could be the essential need of a more offensive approach in anticipation of actions by adversary human networks, along with strengthening the coordinated actions driving to effects aiming to reduce their capabilities. This would unavoidably require integrating activities in both physical and cognitive domains.

Although the design of the improvised explosive devices used in the affected areas has been quite simple, the local and regional security/defence forces have evidenced a poor C-IED performance

Figure 1 – Protests in Mali against France and in favor of Russia in September 2020 (Source: Agencia AP)

and effectiveness, which highlights deficient training, tactics, techniques and procedures. Accordingly, one of the lessons identified is the need of a more comprehensive and effect-oriented approach to C-IED Defence Capability Building when training nations with root problems in skills and materials.

With regards to the improvised explosive devices (IEDs), the trends in the use of commercial-off-the-shelf (COTS) devices for radio controlled IEDs, the adversary use of vehicle borne IED and the emergence of explosive-laden drones (as already used by Russian Private Military Companies, Jama'at Nusrat al Islam wa al Muslimeen JNIM and the Permanent Framework for Defense of Azawad People CSP-DPA at least) as a heritage from Ukraine, are a strong reminder not to forget that C-IED is still essential and to refurbish Allied tactics, techniques and procedures in the path of adequately facing the emerging threats.

In a similar way, as it happened with education and training, the Western forces were strongly focused on "Defeat the Device" matters, while applying a partial understanding/approach to Technical Exploitation, along with a lack of any comprehensive implementation of counterinsurgency and Attack the Networks. This was a limitation for the development of the essential-for-success effects over adversary human networks' capabilities and also over the local population as a key neutral actor.

Accordingly, the opportunity for implementing Attack the Networks approach into C-IED activities has been lost in Sahel: the potential lessons identified would focus on the need of a better analysis on human networks' capabilities, the need of integrating additional proactive actions with the developed reactive actions, and the need of analysis/planning of integrated and synchronized effects over human networks' capabilities.

From the strategic communications' perspective, there was (also is) huge effort in propaganda by both AQ (Al Qaeda) and Daesh-related human networks, in confluence with a poor allied approach to information activities by Western side, along with the already mentioned smart approach to cognitive warfare by Russian actors, which logically drove to our defeat in the information warfare.

As a conclusion, some of the lessons identified are as follows: a need of a good analysis of the human terrain, an effect-based mindset as a must, and an essential requirement for anticipation and

Figure 2 – Captures from a video of CSP-DPA showing how an IED is dropped by a drone (Source: X/Twitter)

Figure 3 – Captures from TIKTOK videos published by ISWAP fighters (Source: www.disinfo.africa)

effectiveness in the cognitive environment. This could all be summarized in the unavoidable need of critical thinking analysis along with a real Attack the Networks approach in operations against non-state actors (which sometimes are also state-sponsored).

References:
C-IED COE internal database
X/Twitter
www.lemonde.fr
www.thesoufancenter.org
www.criticalthreats.org
www.understandingwar.org
www.disinfo.africa

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

PREPARE!

COURSES & TRAINING

Developing Weapons Intelligence Team training for Nations

2024 in a glance...

WIT operators are trained to investigate IED incidents in any environment and to produce standardized tactical, technical and forensic intelligence Level 1 reports to feed the Operations and Intelligence cycle, in order to understand and conduct Attack the Networks' activities more effectively.

From WIT activities and assessment, we can get a Tactical and Technical characterization of an IED event, leading to Pattern Analysis, Tactics, Technics & Procedures (TTPs), Event Signature and Device Profiling.

The C-IED COE is the executing agent for Weapons Intelligence Team (WIT) training for NATO, under the Conference of National Armaments Directors' (CNAD) Voluntary National Contribution Fund (VNCF) mechanism.

Since 2011, the C-IED COE has trained more than 840 Allied and Partner WIT operators (from 47 different countries), supporting Nations in their national WIT capability building process and ensuring Alliance coherence in WIT operations, providing essential Level 1 Exploitation Weapons Technical Intelligence (tactical level) training to teams able to respond to IED incidents – prior to their arrival in an Operational Theatre.

Currently, as part of the VNCF WIT Training 2024/25 Executing Agent Agreement, the WIT courses are held at two different locations: at the Romanian EOD & C-IED Training Base in Râmnicu Vâlcea, and at the Hungarian Defence Forces NCO Academy, in Szentendre, Budapest. During 2024, the first iteration took place between 14 and 31 May in Romania, and the second iteration took place in Hungary between 10 and 27 September. With a duration of three weeks, the course covers

the C-IED Exploitation Level 1 capability, including make-up and type of IEDs, forensics, photography, terrorist tactical design, s-UAS exploitation, DOMEX basic concepts and skills and post blast collection and analysis. The course also includes a very complete practical phase, through which the trainers help develop the skills needed for the

future WIT operators.

The Training Audience for the WIT Course is ideally from Explosive Ordnance Disposal, Engineering, Intelligence, Military Police, Special Operations and Infantry backgrounds.

Additionally, the C-IED COE is responsible for annually hosting the WIT Training Developer Course (TDC). The objective of the course is to educate WIT Course Directors and Senior Instructors in

WIT Course development, by implementing updates on skills and standards, and creating WIT related scenarios, taking into account the risk management, criteria factors for scenario selection, resources management and integration of vignettes.

During 2024, the C-IED COE conducted the WIT TDC between 09 and 13 December 2024, at its premises in Hoyo de Manzanares, Spain. A total of fifteen attendees from eight different nations participated in the course.

For the participating nations, this course is an excellent opportunity to understand the standards, minimum requirements and equipment for organizing a WIT course, as well as the tasks to be

performed by a WIT, risk and resource management, criteria for scenario selection and overall, how to best train their national WIT operators.

What about the future of WIT?

As we can see nowadays in several conflicts taking place all over the world, IEDs continue to be used as a weapon of choice, and not only by insurgents like it was in the past...

In that sense, the fight against the IED system remains relevant, and ensuring the security of troops deployed in theatres of operations will continue to be a primary objective for NATO, by reducing or eliminating the threat posed by the use of IEDs.

Considering its unique capabilities, which 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), the WIT courses will continue to be a relevant capability for NATO Nations and Partners, and the C-IED COE will continue to support Nations and partners in their national capability building process, ensuring the coherence of the Alliance.

DOMEX Course

Collection and Processing in Support to Attack the Networks (DOMEX-AtN) courses. Spain/Hungary.

The C-IED COE successfully completed the second and final iteration of the "DOMEX (Document and Media Exploitation) Collection and Processing in Support of Attack the Networks Course" bringing to completion the iterations as included inside the Programme of Work for 2024. In both iterations, the 12 available spots were filled, receiving more than 60 applications from 11 NATO and partner nations.

The first iteration took place at the C-IED COE facilities in Hoyo de Manzanares (Spain) from 8 to 19 April 2024, while the second took place at the NCO (Non-Commissioned Officers) Academy premises in Szentendre (Hungary) from 26 August to 6 September.

Document and Media Explotation

These courses have a two-week duration: the first one is theoretical-practical, while the second week is primarily practical, with different scenarios and items being exploited.

After completing the course, DOMEX attendees are able to carry out document exploitation (DOCEX), digital media exploitation (MEDEX), cellphone exploitation (CELLEX), and unmanned aircraft system (UAS) exploitation.

Review of the "Attack the Networks" Operational Course (ATNOC)

The C-IED COE carried out a workshop in order to review the ATNOC contents and format, which had been in force for the past 5 years. The main reason for this review was the need to meet actual requirements and to adapt current warfighting concepts to this training.

A total of 7 internal SMEs from the C-IED COE and 3 external SMEs created a very friendly and collaborative environment. The team gathered tactical and operational level expertise and various backgrounds (Intel, C-IED, EOD, MILENG) for the benefit of the overall effort. All tasks and objectives were completely fulfilled.

Attack the Networks Operational Course (ATNOC) is carried on two iterations a year, with around 20/25 students in each one, coming from diverse nations. Supported by internal C-IED COE mentors/briefers and external lecturers from Spain National Police and NATO JFCBS HQ, ATNOC provides AtN related awareness and knowledge to NATO Staff Officers/Senior Staff Assistants from C-IED/Intelligence/Operations/Plans or other counterterrorism related disciplines, from tactical and operational level commands, as well as personnel of Law Enforcement and Intelligence Agencies.

The emphasis is laid on knowledge and skills to integrate and facilitate the comprehensive AtN approach across other HQ processes and disciplines (e.g. plans, intelligence, operations) to recommend lethal and non-lethal ways to engage all networks (adversary, neutral and friendly) and to assess on the engagement effects.

Teaching how to Attack the Networks

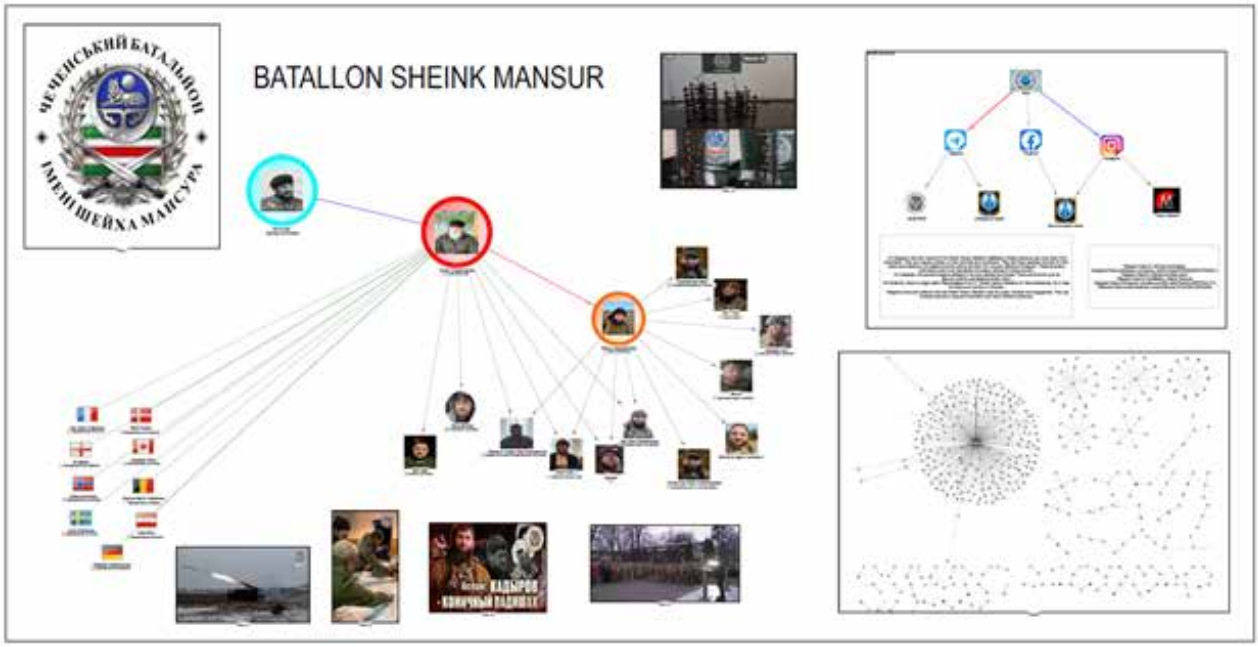
Linking the dots inside the networks

From 4 to 8 November, the C-IED COE hosted the Analyst Notebook Users' Course (ANUC) at its premises in Hoyo de Manzanares.

For participating nations, this type of course is an excellent opportunity to understand the analysis tool developed by i2© and designed to support analysts in their investigations to combat criminal activities. It provides a single environment for users to collate, analyze and share data and the resulting intelligence outcomes.

With Analyst's Notebook, users gain rich visual analysis capabilities that quickly turn complex sets of disparate information into high-quality, actionable intelligence. This helps them and those involved in intelligence analysis identify, predict and avoid criminal, terrorist and fraudulent activities.

With this course (held twice a year) the C-IED COE continues to support military and law enforcement organizations in their analyst capacity building process.



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

C-IED ON THE FIELD!

EXERCISES

Loyal Leda 2024 (LOLE24)

Exercise LOYAL LEDA 2024 (LOLE24) is a LANDCOM-sponsored land domain tactical-level Computer Assisted Exercise/Command Post Exercise (CAX/CPX) aimed to train and evaluate Rapid Reaction Corps - France (RRC-FR) in a Warfighting Corps HQ role as well as up to two Corps HQs being Multinational Corps Northeast (MNC-NE) and 1st German- Netherland Corps (1GNC), at MJO+ scale against a peer adversary in NATO Strategic Direction North-East.

The C-IED COE supported Loyal Leda 24 at NATO JFTC (Joint Force Training Centre) in Bydgoszcz, Poland, from 5 to14 March 2024 in order to provide support to JFTC with the implementation of C-IED approach in the exercise and to challenge the training audience with full spectrum C-IED in a conventional warfighting scenario.

Northern Solution 2024 (NS24): a C-IED exercise

The C-IED COE successfully conducted Northern Solution 24 at Keflavik Airbase, Iceland, from 24 September to 4 October. Held in conjunction with Northern Challenge 2024 (NC24), the exercise provided NATO staff officers with realistic training to combat threats from improvised explosive devices (IEDs), reinforcing NATO's operational capabilities in a multi-domain environment.
The integration of NS 24 into NC 24 created an authentic training environment for participants from the United States, Canada, Spain and the Netherlands.

Valiant Blaster 2024

Supporting Marine Brigade to build C-IED capabilities

The C-IED COE supported the exercise Valiant Blaster 24, organized by the Spanish Marine Brigade in San Fernando (Cadiz, Spain) to maintain and improve the EOD (Explosive Ordnance Disposal) capabilities needed in the C-IED fight.

Theoretical session with an EOD expert from the C-IED COE

The exercise included EOD units from Spanish Armed Forces (Navy, Army and Air and Space Forces) and Allied countries, as well as personnel from diverse law enforcement agencies. Its main objective has been to promote, strengthen and increase interoperability between the various EOD units, as well as to share TTPs (Tactics, Techniques and Procedures) and best practices, with special emphasis on Defeat the Device within the three pillars of the C-IED fight.

The C-IED COE, as a reference centre in the discipline, has supported the exercise with the participation of experts from the “Defeat the Device” area. It has also provided participants with an updated conference on the different emerging threats in the various theatres of operations where the Spanish Armed Forces and Allied Armies currently carry out their missions.

EOD operator in a practical exercise

Through the preparation of realistic scenarios, thanks to the data collected in areas of operations, activities have been carried out where participants have faced a wide variety of IEDs (commanded, activated by the victim, suicide vests, car bombs, among others) and have been able to put into practice the usefulness of various TTPs, integrating EOD practices, level 1 technical exploitation and the work of the WIT team and the CCEOD (Explosive Ordnance Disposal Control Centre) in the intelligence cycle.

ADDING C-IED PERSPECTIVE

CONFERENCES, SEMINARS AND WORKING GROUPS

C-IED in support to NATO Cognitive Warfare Initiative

Inside its Warfare Development Agenda, the Alliance is developing the NATO Cognitive Warfare (COGWAR) Concept, supported by several Subject Matter Experts across NATO structure and the academic community. The first draft was submitted to Allied Command Transformation (ACT) last May 2024 and in this document, the C-IED COE is mentioned as part of the "large community of interest".

The role of this C-IED COE has been very proactive regarding the matter. The Centre has participated, not only providing inputs, but also initiatives like the COGNITIVE AUGMENTATION FOR MILITARY APPLICATIONS NIAG SG (NATO Industrial Advisory Group – Study Group) 278 during 2023 and the Technical Report of the Human Factors and Medicine (HFM), Evaluation Criteria and Use Cases for Information Operation/Social Media Simulators, Exploratory Team Number 212 (NATO STO-TR-HFM-ET-212) during 2024.

From the academic point of view, we have attended the HFM 361 Mitigating and Responding to Cognitive Warfare celebrated in 2023 and the "Cognitive Warfare Course" first edition, hosted by the Crisis Management and Disasters Response COE (CMDR COE) during the summer of 2024. One of our pillars (the main one) is Attack the Networks, which focuses on how to deal with friendly and neutral human networks, as well as adversary ones. Because of this, it is important to effectively comprehend the operational environment, particularly if there is a potential threat from improvised explosive devices (IEDs) nearby.

The Alliance divides the supporting concepts into four categories: SHAPE, PROTECT, COLLABORATE & EDUCATE. The Alliance views COGWAR as a "whole culture problem" because the adversaries' cognitive attacks impact both domestic and Joint Operations Area (JOA) audiences.

In order to carry out our duties, the C-IED COE efforts focus on EDUCATION and COLLABORATION, so we participate in forums that enhance our knowledge, we join SME (Subject Matter Expert) networks (even outside of the NATO setting) and, most importantly, we implement the COGWAR concept in our specific courses.

In parallel, we continue tracking different adver-

sary human networks using IEDs across the world, based on NATO or Sponsoring Nation's interests (following our Programme of Work). Then, we disseminate these comprehensive reports to the community, with special focus on human networks' dynamics, their tactics, techniques & procedures. All of this without neglecting the technical aspects of the devices and taking into account the activities in the cyberspace of the documents from those adversary human networks alone or even sponsored by state actors.

3D Technology on modern conflicts and its implementation in C-IED efforts

During the past years, 3D printing has gained increased relevance on how we confront armed conflicts. 3D printing has provided strategic benefits to us, but it has also smoothed the way for non-state actors, like insurgent groups, to adopt open-source technologies to develop components for improvised explosive devices (IEDs).

These technologies have demonstrated their value, particularly during wartime in the conflict in Ukraine and across regions in the Middle East, by producing crucial parts and equipment on the frontlines, as well as copying weapons.

It is becoming more and more common for military forces and insurgent groups to use additive manufacturing, according to various reports from official sources and academic studies. This has forced Allied forces to develop faster and more advanced countermeasures, which shows how important it is to take a proactive approach and control access to these technologies. The ability of 3D to replicate critical components of captured IEDs has helped NATO forces anticipate new threats and design more effective defenses.
In this article, we will look at how 3D printing has impacted today's battlefield and examine a project led by NATO's Counter-IED Centre of Excellence (C-IED COE) over the past year that focused on developing 3D-printing and scanning capabilities.

One of the main places where 3D printing has taken on new applications is the Ukraine conflict. Both military and paramilitary organizations have been using 3D printers to quickly generate spare parts, create drones and, at times, reproduce ammunition and IEDs. The use of open-source technologies and the access to local materials has enabled these actors to create tactical solutions in real time to meet the demands of combat. In

particular, this technology has given local forces a flexibility advantage, allowing them to adapt their capabilities as enemy tactics evolve.

In addition to tactical benefits, 3D printing has also solved critical logistic challenges. By manufacturing spare parts for military equipment on-site, armed forces have reduced their reliance on long supply chains, which are often vulnerable to disruption. This approach enables greater operational autonomy and ensures that units in the field can continue operations without substantial delays.
In the Middle East, additive manufacturing has also been used to improve logistics capabilities, enabling the manufacture of tools and spare parts for military equipment, reducing the need to rely on vulnerable supply chains. However, one of the most troubling uses has been the production of key components for IEDs and improvised weapons, prompting NATO forces and other Allies to develop advanced technological countermeasures, including the ability to replicate these devices for study.

To improve how units fight IEDs, the C-IED COE has bought and used some new and improved 3D-printing and scanning tools. These technologies have been key for duplicating and examining threats in multiple conflict situations, enabling NATO forces to understand and manage risks in real time.

The 3D printer Markforged Mark Two (Gen 2) relies on Fused Filament Fabrication (FFF) technology. Parts from nylon or onyx that have fibreglass, Kevlar or carbon fibre reinforcements can be printed with it. This printer has been invaluable for making large and medium copies of IEDs and other military field items, particularly in Ukraine. Even without the best resolution of alternative resin printers, its toughness and adaptability allow for outstanding functional and sustainable prototypes. This printer has some impressive technical features, including:

- Printing area: 320 x 132 x 154 mm.
- It works with nylon, onyx, carbon fibre, fibreglass and Kevlar.

This printer enables accurate replication of medium-sized artifacts, giving military units a significant advantage in studying threats in the field.

Formlabs FORM 3+ is a resin 3D printer that applies stereolithography (SLA) technology to create prints with very high detail. Using the printer in this project enables precise reproduction of small parts, including fuses and internal elements of explosive ordnance. Its ability to print at extremely fine layer resolutions has been instrumental in studying the detailed structure of IEDs captured or identified in conflict zones.

The accuracy of the Formlabs FORM 3+ has been vital in creating exact replicas of critical components, enabling forces in the field to anticipate potential threats and design more effective countermeasures.

The Shining HX is a high-precision portable 3D scanner designed to capture medium to large objects. This device has been used by our teams to scan projectiles, aviation bombs and IEDs. Its portability and accuracy make it an ideal tool for field work, allowing EOD and WIT teams, or even other field units, to obtain detailed 3D models of objects of tactical, operational or strategic interest without the need to remove them from the area of operations.

- Scanning resolution: up to 0.05 mm.
- Scanning volume: from 300 mm to 4000 mm.
- Scanning modes: structured light and infrared laser.

With its ability to operate in a variety of conditions and easy portability, the Shining HX significantly improves real-time data collection, allowing 3D models of IEDs to be quickly sent to a centralized database for analysis.

The Shining TrakScan is a high-precision fixed scanner, ideal for use in a laboratory to capture small and medium-sized objects. This scanner has been designed to obtain extremely detailed 3D models of objects recovered from the battlefield, allowing their exhaustive study under controlled conditions.

- Accuracy: up to 0.01 mm.
- Scanning area: up to 250 mm.
- Scanning speed: 2 million points per second.

This fixed scanner complements the portable scanner, providing additional capacity for detailed scanning of small artifacts.

The key feature of the project is the design of a substantial database to archive, retrieve and manage the 3D images and data produced by the 3D scanning technology. Right now, this centralized database is just a proof of concept (PoC) of the C-IED COE. However, it is important to highlight that it would enhance how the information is currently shared among all NATO members, improving both decision-making and adaptiveness to developing threats.

The current project aims to reach future functionalities that will include:

- Real-time updates and immediate access: the database would be updated in real time with 3D scans obtained from operations in different theatres of conflict. This grants that each NATO member would have access to recent information, which is necessary for efficient and rapid decisions.
- Interoperability: created for operability on numerous platforms and devices, the database would support collaboration among units that are geographically separated, thus enhancing partnership among Allied nations.
- Security measures: the database would feature information protected by solid encryption systems alongside rigid access controls that will guarantee data security and integrity on an ongoing basis, thus stopping unauthorized access.

Strategic benefits of the database:

The design of this database would provide important strategic advantages for NATO operations:

- Improved situational awareness: providing rich visualizations of threats, this database would play a role in increasing situational awareness for forces, making operations in the field safer and more effective.
- Training and simulation: due to the real-world data it handles, the database would allow the development of quite accurate training modules and simulations, preparing the forces for the obstacles they could encounter in the field. This instrument would prove to be essential for training

with a tactical focus and the design of operational approaches.

- Historical archive: in addition, the database would act as a repository of past threats, allowing the data to be analyzed to identify patterns and trends. This capability would facilitate the development of more robust defense strategies in the future.

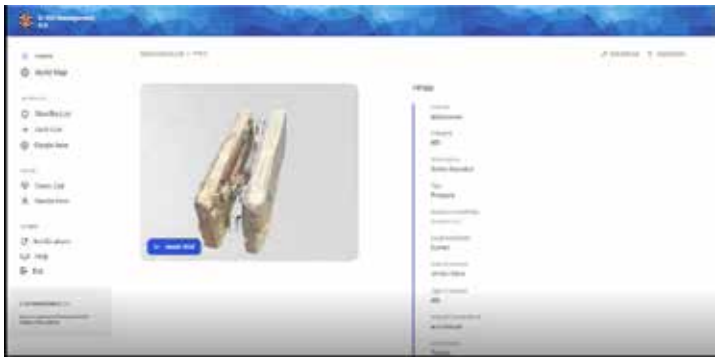
The most notable feature of the database is its ability to store and share 3D threat models in formats such as .stl, .fbx and .obj. These models can be downloaded, analyzed and, if necessary, printed by other Allied units, allowing a detailed study of the captured artifacts. Descriptions, images, documents and videos can also be attached to each model, providing a complete and accessible view of each threat.

To encourage collaboration and information sharing among users, one of the features will be a discussion forum where community members could comment and contribute with additional information on explosive threats. This forum will allow the exchange of knowledge and experience in real time, improving the accuracy and usefulness of the data contained in the database.

As advances in additive manufacturing and 3D scanning continue to occur, fresh obstacles come to light, one of which being the requirement for process standardization and the handling of large volumes of data in a timely manner. The C-IED COE, along with other NATO organizations, is working hard to create cohesive protocols and build secure communication networks so that these technologies can more effectively integrate into the military field.

Conclusion

3D printing, together with high-precision scanning, has confirmed its importance as a key method for studying and reproducing threats on the battlefield. Although this has enabled non-state actors to exploit open-source technologies in the creation of their own explosive devices, it continues to drive Allied forces to continuously design rapid and progressive countermeasures. Through projects such as this, the C-IED COE seeks to enhance the capabilities of NATO forces, enabling a faster and more effective response to evolving threats, and contributing to global security in the fight against IEDs.



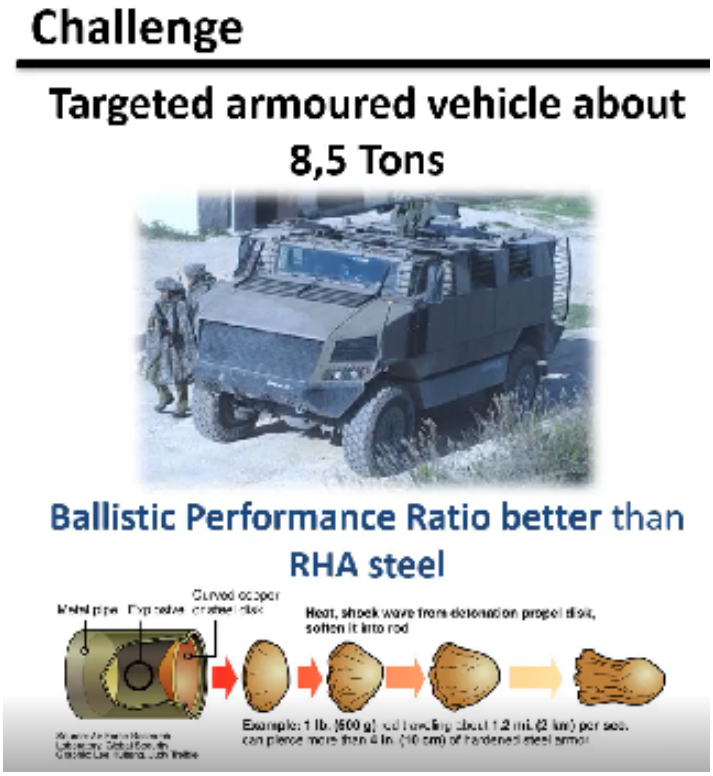
AKHENATON Project

Design of an Add-On Armour (AOA) to protect light military vehicles

An EFP-IED (Explosively Formed Projectile - IED) is one of the terrorist weapons of choice according to the information gathered from a diversity of scenarios during last years (Syria, Iraq, Lebanon, Yemen, Afghanistan, Mali, Nigeria, Kenya, Bahrain and Egypt). In particular Iraq, Yemen and Syria conflicts exemplified how effective can Radio-Controlled camouflaged EFP-IED lateral attacks be against light vehicles. Permanent reinforced lateral armours would increase the total vehicle weight in all tactical situations, including those where they are not required, affecting its mobility and other features. Akhenaton Research and Development outcomes were oriented to fill this gap with a few add-on alternatives against EFP-IED lateral attacks.
The overall goal of this project was to achieve a significant impact on NATO doctrine and practices in this matter, through the conceptual design, testing and experimentation of cost-effective (in terms of ballistic protection with mass efficiency above RHA (Rolled Homogeneous Armour) steel) advanced material add-on armour to protect light tactical vehicles (<10 tons) from characterized 100 mm (High-Explosive charged) EFP-IED lateral attacks preserving its high-mobility and endurance.

Akhenaton development involved three nations (Spain, Portugal and Germany) and several stakeholders tackling a range of topics like design, experimentation, manufacture, procurement, modelling and simulation.

Apart from the C-IED COE sponsorship, Akhenaton gathered expertise from military units (International Demining Centre), academia (Universidad Politécnica de Madrid and Universidade do Minho), research institutions (Fibrenamics), intelligence agencies (BKA) and experienced companies (Urovesa and E&Q).



WORK DONE

The logic of the project divided the tasks into two differentiated blocks, being 2022 mainly focused on preliminary discussions among the partners and on setting up several supports required to execute the design, procurement and experimentation activities, also considering the different partners' views. The second block of activities performed during 2023 was oriented to the experimental approach as the fundamentals for design, modelling and simulation.
The first quarter of 2022 was focused on tasks

planning, main discussions about the threat, candidate material and AOA design scope, concentrating the highest number of technical meetings. The second quarter of the year included the first deliverable (state-of-the-art). In the second half of the year, several deliverable reports (on design and testing) were issued. Major testing campaigns were conducted during 2023, when the main milestones were achieved.

RESULTS AND MAIN INSIGHTS

After the corresponding iterative process through the different tasks of the project, the design of the AOA mock-up was refined and optimized enough to cope with the requirements of protection and mobility defined at the beginning of the project, complying with the mass efficiency required for the combination of materials to protect against the threat.

Thanks to the experimental campaign, the procurement process of the necessary materials was identified as one of the major takeaways of the project. In that sense, the proper management of the supply chain became critical for the experimental approach to validate and refine a protection armour design.

Modelling and simulation activities were also paramount for the success of the project. All the data gathered during the experimental campaign were used to refine and further tune-up the design by extending and extrapolating material behaviour.

CONCLUSIONS

- AOA design mocks protect light vehicles from the threat preserving their mobility, which is a good outcome to foster comparable solutions for similar EFP-IED threats. The experimental-based design approach can benefit other IED ballistic mitigation projects in NATO and the lessons identified in the following methodological aspects could serve as means for learning:

- AOA experimental design is fully linked to procurement workflows and material availability.

- AOA multi-layer mocks layout to be shot is decided on-site (qualitative analysis on previous shots).

- AOA testing firing sequences in the planning phase (logical trees on which mock to shoot) help to save the remaining material and to optimize the procurement costs.

One additional lesson identified is that one of the main critical factors for the development of the project was the challenge to put together the resources required for experimentation. In case of testing recurrence, local units would require an organic experimental team supporting the field tests. This will help to gather needs from the different branches and build up expertise in the procurement and complexity of field test resource management.

Further work can be done identifying EFPs with similar RHA-e risk level by AEP-55 (Allied Engineering Publication 55) analysis. This could help the NATO community of interest to group homemade EFP-IED and match them to NATO Standards. A related STANREC (Standard Recommendation) could also be an initiative to tackle in the short term. Moreover, the identification of similar EFP-IED in theatre and even higher-level threats (i.e. bigger EFP-IED calibre) could benefit from the results of Akhenaton and exploit its lessons for threat level awareness.

Supporting Tunisia's C-IED capabilities

A group of experts from the C-IED Centre of Excellence (C-IED COE) were supporting through technical advisory the North Atlantic Treaty Organization (NATO) Science for Peace and Security (SPS) sponsored initiative on C-IED Defense Capability Building (DCB) for Tunisian Armed Forces from 26 to 29 February 2024 in Bizerte, Tunisia. The referred initiative is based on the essential and expert support from five NATO nations (France, Germany, Spain, United Kingdom and United States) which are members of the Steering Group for the project, chaired by Tunisia.

The main focus of that DCB initiative is centred in the development of the Tunisian C-IED Centre of Excellence (TC2E), founded in 2022 inside the Tunisian Army Base "Menzel Jemil" in the nice coastal and historical city of Bizerte.

TC2E is evidencing a highly professional approach to the development of Tunisian's own national C-IED capabilities, mostly answering to the lowly known threat they are suffering from terrorist groups (almost 100 IED incidents took place last year in Tunisian territory).

Training on Unmanned Aircraft System's Technical Exploitation

The C-IED COE provided specific training on Technical Exploitation on Drones in the benefit of the Hungarian Armed Forces. The initiative comprises both Threat Update and Technical Exploitation on Explosive-Laden Drones, including DOMEX. The referred initiative has boosted the identification of that specific gap in NATO and the related development of the C-IED COE's experiment on "Threat Analysis, Risk Assessment and Technical Exploitation on Explosive-Laden Drones" during 2025.

Alternate Threat Scenarios (ATS) Seminar series

Under the sponsorship of the North Atlantic Treaty Organization (NATO) Headquarters' Emerging Security Challenges Division (ESCD) Defence Against Terrorism (DAT) Programme of Work (PoW), the NATO-Accredited C-IED Centre of Excellence has organized two consecutive editions of the "Alternate Threat Scenarios Seminar (ATS)" in Madrid.

The aim of the ATS Seminars is to provide a favourable space to present alternate (so those emerging, unprecedented, never directly faced, unexpected or modified from current ones) models for threat scenarios as developed by non-state actors, just in benefit of critical thinking analysis.

The main topics for the ATS Seminarsare focused on Alternate scenarios based: on terrorist threats still not conducted, on unexpected violent actions, on actors unidentified as adversary ones, on effects over critical infrastructure, on effects over mass events, on second and third order effects, on own unidentified vulnerabilities, and on traditionally unprotected events/interests.

In fact, ATS editions have been dealing with different alternate threat scenarios as follows:
1) Analysis on a potential attack over a military or commercial vessel using explosive atmospheres and 3D-printed weapons.
2) Analysis on a potential attack over a military or commercial airplane using hard-to-detect precursors and highly exothermic-reactive chemicals to sabotage the landed airplane or to destroy it at the highest cruise altitude.
3) Analysis on a potential attack over a military compound or critical infrastructure, combining the use of modified commercial or homemade drones with incendiary devices aiming to create a planned hard to extinguish arson, in the aim of burning huge forest areas surrounding the targeted facilities.
4) Analysis on a potential attack over a military or commercial vessel with a homemade explosive-laden unmanned underwater vehicle (UUV).
5) Analysis on a potential attack over a military or commercial airfield/airport/base with a combination of explosive-laden, incendiary and hoax balloons.
6) Analysis on a potential attack over a civilian building through creating an explosive atmosphere with natural gas installation.

C-IED Interagency Workshop

Entitled as "Understanding Threat Dynamics, Anticipating Threat Evolution, Seeking Interagency Effects", the last edition of the C-IED Interagency Workshop (IAWS) was focused on a comprehensive approach to the hybrid threat environment in which Countering Improvised Explosive Devices (C-IED) poses an essential contribution against the threats. The three-day event was structured as follows: (Day 1) Update on Threat & Dynamics from non-state actors, (Day 2) Intelligence contribution to Attack the Networks & Cognitive Warfare, (Day 3) Prospective on Threats as derived from non-state actors.

The diversity of the briefings ranged from an overview on the current situation of Improvised Explosive Devices (IED) threat, and the adversarial tactics, techniques and procedures, through a consideration on the hybrid scenario evolution and emerging threats. A final prospective vision was given to the audience as a closing opportunity to encourage future collaborations with an interagency mind-set.

Among the most relevant conclusions drawn from the discussions, the following ones can be highlighted:

- To face a quickly evolving hybrid threat environment, both updated and effective tools/procedures, along with a multidisciplinary perspective are needed.
- Those tools, applied not only to IED events, but also to face the overall threat from non-state actors, would need to adopt an adaptive, holistic and flexible approach.
- Smart information sharing continues being essential for an effective fight against the multidimensional and multinational spirit of current and future threats.

Supporting UN in the development of C-IED

The inaugural United Nations Combined Review EOD / Counter-IED Guidance Documents Writing Workshop (WS) took place from 12 to 16 February at the SWISSINT (Swiss Armed Forces International Command Training Centre) Academy in Stan, Switzerland.

Organized by the United Nations Office of Military Affairs, the workshop brought together Member States, EOD Subject Matter Experts and international police organizations to collaboratively review and develop revised drafts of key documents related to Explosive Ordnance and Counter-Improvised Explosive Devices (C-IED).

This was the second writing workshop and it was focused on the UN Peacekeeping Missions EOD Unit Manual dating September 2017 and its alignment with the already developed draft of the revised Improvised Explosive Device Threat Mitigation Handbook from December 2023.

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 DEVICE IED SYSTEMS"

VISIT: ciedcoe.org

NATO OTAN
ACCREDITED COE

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

LATEST C-IED C

In order to share the knowledge on C-IED matters, our

First, we would like to mention the handbook "Attack the Networks Procedures for Support to Effects and Ta from C-IED/Attack the Networks' perspective, its content includes not only the adaption of current tools, tacti ment and assessment, but also the development of new tools and procedures as "AMATE" (Attack the Netwo assessment, as well as to recognition, analysis, validation a

Regarding reports, we are pleased to ha

Threat Analysis:

- DAESH Handbook series on the offensive use of commercial-off-the-shelf (COTS) drones.
- DAESH-related RocketChat group sharing online instructions for 3D-printed firearms manufacture.
- Migration of DAESH followers to alternate instant messaging platforms.
- South American DAESH followers are sharing online instructions for homemade explosives (HME) manufacture through RocketChat.
- TELEGRAM account sharing online instructions for homemade explosives (HME) and improvised explosive devices (IED) manufacture with DAESH followers.
- ARABIC SEA/RED SEA - Update on threats to maritime traffic.
- Ansar Allah/Houthi rebels' threats over navigation through the Red Sea and Arabian Sea.
- Resurgence of Chechen group "LAMANHO" through RocketChat.
- Detonations of electronic devices in Lebanon.
- Update on Hezbollah's use of explosive-laden drones.
- Use of explosive-laden drones and other improvised explosive devices by Palestinian militias in the attacks against Israel from Gaza Strip.
- Analysis of online distributed "How to IED" video.
- Explosively Formed Penetrators (EFP) for First Person View (FPV) drones in Ukraine.
- Trends in the use of first-person view explosive-laden drones in Ukraine conflict.
- Ukraine – Manual on modification of conventional munitions for explosive-laden drones. Pro-Russian handbook on insurgency tactics.
- Russian handbook on improvised TTP with hand grenades.
- Russian TELEGRAM sharing online instructions for explosive manufacture.
- Russian handbook on explosive-laden FPV drones.
- Dynamics on Wagner Group's role in Africa and Ukraine.
- Implications from Wagner Group training support to Belarus (BLR).
- Wagner Group Ground Force Commander.
- Wagner Group Access strategies to areas of operations.
- Wagner Group as a global actor.
- Wagner Group Training and Recruitment.
- Wagner Group Splitting.
- Russian manual on Ukrainian tactical use of FPV drones.
- Pro-Al Qaeda group publishes manual for homemade explosives.
- Pro-DAESH LAMANHO group published homemade explosives manual.

Should your organization be part of the C
receive our products, please subs

OE PRODUCTS

r COE has distributed several products in the last year.

arget System Analysis over Non-state Actors and other Human Networks". Using a comprehensive approach ics, techniques and procedures in support to human network analysis, support to targeting, network engage- rks Matrix for Analysis in support to Target Entities/Audiences Engagement) in direct support to vulnerability and prioritization of potential targeting entities/audiences.
ve finalized and published the following:

Events:

- 10th Lessons Learned Workshop 2024 .
- 6th Technology Workshop 2024 .
- 6th Interagency Workshop 2023.
- Technical Exploitation in Water Environnent 2024 Seminar & Trials.
- Alternate Threat Scenarios 2023 Seminar.

Projects:

- C-IED/ATN Integration Experiment 2024.
- Advanced Document, Media and Cellular Exploitation (A-DOMEX).
- AKHENATON.
- Northern Solution 2024.
- Handbook on procedures for support to effects and target system analysis over non-state actors and other human networks.
- Attack the Networks Matrix – Analysis on Targets/Audiences for Effects (AMATE) tool .

Protection:

- Russian improvised passive protection/mitigation measures on airplanes against explosive-laden drones.
- Russian improvised passive protection/mitigation measures. Connecting Technical Exploitation with Intelligence outputs & outcomes from Attack the Networks (AtN) perspective.

Other:

- Analysis of explosive-related content: Deep Web - Drug Market "Breaking Bad".
- Non-state actors' Tactics, Techniques and Procedures (TTP) Update January 2024.
- UKRAINE – Manual on modification of conventional munitions for explosive-laden drones.
- Management - 2023 Annual Quality Assurance Report.
- Human Network Dynamics - Daesh in Khurasan Wilayat: transnational vision and threats to Europe.

-IED Community of Interest and would like to
mit your request to info@ciedcoe.org

Soldier in the Spotlight

Major (Marines) Juan Manuel Mancilla, PhD

BRAVE BY LAND AND SEA! (¡Valientes por tierra y por mar! – Spanish Marines motto)

Major Juan Manuel Mancilla is one of the most experienced members in our Centre. We have asked him several questions to find out more about his educational path, his professional career and how he ended up in the fight against IED:

You joined the Spanish Armed Forces after obtaining a university degree. Which studies did you pursue and how did you first get interested in the military?
After finishing my undergraduate studies and earning a Bachelor of Science, I completed my mandatory military service in the Spanish Navy Maneuver and Navigation Specialists Corps as an Ensign. During that time, I discovered the incredible work and history of the Spanish Marines and my calling awoke.

Were your first postings related to the fight against IEDs?
Given the complexity of the C-IED fight and the necessity for a wide range of complementing skills, some experience is required before becoming competent in the area. My initial postings were in infantry, artillery and military police units, which were not directly related to C-IED, but they gave me the necessary experience to better comprehend it. After becoming an EOD officer, I was able to work in the C-IED arena, assisting Intelligence Analysts through technical assessments.

What kind of training did you follow in this area?
Once stationed in the C-IED COE, I had the opportunity to be educated as a C-IED Staff Officer. Due to my EOD expertise, most of the training I received was focused on technical exploitation and the manufacture and neutralization of homemade explosives. These training possibilities enabled me to earn a Mining Engineering PhD, focusing on the production, characterization and modelling of homemade explosives.

In the middle of your military career, you applied for a leave of absence in order to work at a civilian organization. Could you explain how this period was?
I had the great opportunity to work for the World Customs Organization (WCO) for over three years as part of the South-East Asia and Pacific Islands Security Project. This project was a truly instructive experience for me, both personally and professionally. It included several C-IED related sub-areas, such as the control of the illegal trafficking of small arms and light weapons or the control of chemical precursors used to manufacture homemade explosives. It also helped me to learn about how other international organizations work in C-IED-related topics.

Why did you return to the C-IED COE?

I believe that joining the C-IED COE is a natural progression for someone who wants to work in the EOD/C-IED arena, in a multinational environment, with real experts from different countries. This is what the C-IED COE provides to its members. What I found during my first tour was far better than what I expected and this motivated me to return to the unit following my experience at the WCO.

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

I have mostly worked in the field of technical exploitation, working as the course director for the Weapons Intelligence Team (WIT) first and the Document and Media Exploitation Course (DOMEX) now. In addition to that, I assist my colleagues with any other needs that might arise, usually providing technical support for the reports of intelligence analysts.

How do you assess these years of service at the C-IED COE?

Outstanding! Both on a personal and professional level, the C-IED COE has allowed me to grow and gain experiences that I would probably not have been able to obtain in other units. If I could go back in time to that moment when I first applied for a position at the C-IED COE, I would apply again. I believe this explains everything.

What professional challenges do you pose yourself for the future?

I would like to consolidate the project I am currently leading, which is the DOMEX training package, and once achieved, I would like to take on new challenges that will allow me to continue growing. In a constantly moving world, those who stand still get left behind.

Major Mancilla during one of the DOMEX courses

UPCOMING EVENTS 2025

C-IED COE courses and events planned for 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.

UPCOMING E	
Date/Place/Course	
03-07 FEB/ESP/Analyst Notebook Users Course (ANUC) 25.1	15 seats available
24-28 FEB/ESP/C-IED Staff Officer Course (CSOC) 25.1	24 seats available
04-06 MAR/ESP/Anual Discipline Conference (ADC)	
31MAR-11 APR/ESP/AtN Operational Course (ATNOC) 25.1	24 seats available
05-09 MAY/ESP/Analyst Notebook Users Course (ANUC) 25.2	15 seats available
12-30 MAY/ROU/NATO Weapons Intelligence Team Course (WIT) 25.1	20 seats available
19-30 MAY/ESP/Document and Media Exploitation Course (DOMEX) 25.1	12 seats available
09-13 JUN/ESP/C-IED Annual Conference 2025 (CIEDAC25)	
23-27 JUN/ESP/C-IED Staff Officer Course (CSOC) 25.2	24 seats available
01-19 SEP/HUN/NATO Weapons Intelligence Team Course (WIT) 25.2	20 seats available
29 SEP-03 OCT/ESP/Analyst Notebook Users Course (ANUC) 25.3	15 seats available
20-24 OCT/ESP/C-IED Staff Officer Course (CSOC) 25.3	24 seats available
TBD/ESP/Advanced DOMEX Course	10 seats available
TBD/ESP/DOMEX Train the trainers Course	8 seats available/M
17-28 NOV/ESP/AtN Operational Course (ATNOC) 25.2	24 seats available
01-05 DEC/ESP/NATO Weapons Intelligence Team Training Developer Course (WIT TDC)	12 seats available

NOTE:

1. The events indicated in red are identified as the C-IED COE's DIAMOND EVENTS.

2. The proper "SAVE THE DATE" and "CALLING LETTER" for each event will be released in advance.

EVENTS 2025

Availability	Duration	Details
/Military, Law Enforcement & civilian analysts	5 days course	Not classified, no fee
/C-IED SO and Senior SA	5 days course	NATO Approved, no fee
/C-IED SO and Senior SA	10 days course	NATO Approved, no fee
/Military, Law Enforcement & civilian analysts	5 days course	Not classified, no fee
/OF 1-3 and OR 4-8	13 days course	NATO Approved, 125€ (for non-VNCF) (TBC)
/Open to military	10 days course	NATO Listed, no fee
		Not classified
/C-IED SO and Senior SA	5 days course	NATO Approved, no fee
/OF 1-3 and OR 4-8	13 days course	NATO Approved, 125€ (for non-VNCF) (TBC)
/Military, Law Enforcement & civilian analysts	5 days course	Not classified, no fee
/C-IED SO and Senior SA	5 days course	NATO Approved, no fee
/Military, Law Enforcement & civilian analysts	5 days course	NATO Listed, no fee
Military, Law Enforcement & civilian analysts	5 days course	No fee
/C-IED SO and Senior SA	10 days course	NATO Approved, no fee
/C-IED SO and Senior SA	5 days course	

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