ISSN 2050-6732 (Print)
ISSN 2050-6740 (Online)

Counter-IED Report

Spring/Summer 2025

NATO OTAN

AMO

RK Consulting (EOD) Ltd

Second Floor Strategies

SmartRayVision®

Premium X-Ray Technology

Extreme 3X Dual System

AI SMART | RUGGED | DEPENDABLE

AI

IP67 PROTECTION

50°C 29.44°C

Compatible

877.638.3868 | sales@smartrayvision.com | www.smartrayvision.com

EDITORIAL AND TECHNOLOGY PARTNERS

MEDIA PARTNERS

Counter-IED Report
Published by Delta Business Media Limited
167-169 Great Portland Street, 5th Floor
London, W1W 5PF
United Kingdom

Tel: +44 (0) 20 7193 2303
info@deltabusinessmedia.com
www.counteriedreport.com

ISSN 2050-6732 (Print)
ISSN 2050-6740 (Online)

The opinions and views expressed in the editorial content in this report are those of the authors alone and do not necessarily represent the views of any organisation with which they may be associated. Material in advertisements and promotional features may be considered to represent the views of the advertisers and promoters. The views and opinions expressed in this report do not necessarily express the views of the publisher. While every care has been taken in the preparation of the report, the publisher is not responsible for such opinions and views or for any inaccuracies in the articles.

CONTENTS

ICOR TECHNOLOGY

MED-ENG®

TOGETHER, WE SAVE LIVES

Med-Eng and ICOR are now part of the same team and share a unified purpose: Develop, build and support best-in-class equipment for Military and Public Safety end users. To learn more, please contact your authorized representative.

icortechnology.com / med-eng.com

CONTENTS

NATO EOD Demonstrations & Trials 2025

NATO OTAN

SLOVAKIA

EXPLOSIVE • ORDNANCE • DISPOSAL ★ CENTRE OF EXCELLENCE ★

NATO EOD DEMONSTRATIONS AND TRIALS

8-9 OCTOBER 2025

INCHEBA EXPO BRATISLAVA, SLOVAKIA

"EOD Technologies in NATO Multi-Domain Operations"

www.eodcoe.org


SAFE PRO GROUP
Safety with Confidence
REAL WORLD DETECTIONS IN UKRAINE
1,290,679
Images Processed
23,286+
Landmines & UXO Detected
5,338
Hectares Surveyed
18
Data Analyzed (TB)
NASDAQ: SPAI


SMART PORTABLE X-RAY SOLUTIONS
VIDISCO
DISCOVER WITH CONFIDENCE
security@vidisco.com
vidisco.com

FOREWORD

By Rob Hyde-Bales, Consulting Editor, Counter-IED Report

As we commemorate the 80th Anniversary of the end of the Second World War in Europe on 8th May 2025, the bloodiest and the largest war in the world's recent history, conflict continues in many areas of the world. In Europe war has returned after Russia's invasion of Ukraine in February 2022. In the Middle East, Israel remains mired in Gaza in its efforts to defeat Hamas after its attacks on Israel in October 2023. Most recently, tensions have flared up again between India and Pakistan – two nuclear armed nations – after the deaths of Indian tourists at the hands of suspected Pakistan based militants in the disputed territory of Kashmir in April this year.

EUROPE

Russia-Ukraine conflict

One of the major sources of conflict in the world today remains the bitter war between Russia and Ukraine. The initial conflict which erupted 11 years ago in Donbas region was sparked by a political unrest in Ukraine and Russia's annexation of Crimea during the power vacuum in the weeks after the Euromaidan Revolution in March 2014. After a full-scale Russian invasion in February 2022, it remains one of the most complex and defining issues in world politics today. After more than three years of hostilities, Russia now occupies some 20% of Ukrainian territory including Crimea.

As a result of heavy fighting 30% of the Ukrainian territory is potentially contaminated with landmines, unexploded ordnance (UXO), and improvised explosive devices (IEDs). The most affected regions include Kharkiv, Kherson, Donetsk, Luhansk, Zaporizhzhia, and Mykolaiv regions. NGOs like HALO Trust, MAG, and FSD are conducting clearance operations in safer areas. USA, EU, Japan, Canada, and other international donors have provided funding, equipment, and training; mine risk education is being rolled out in schools and rural communities. Modern technologies, such as drones and remote-sensing are being used to map minefields along with ground-based robotic demining systems and metal detectors; AI-assisted tools are used to improve detection speed and accuracy in clearance operations. In the Kursk region of Russia, which borders Ukraine, demining and UXO disposal operations are also underway following heavy fighting during Ukraine's nine-months incursion.

Since the start of Russia's full-scale invasion of Ukraine, there have been a number of high-profile assassinations in Russia using improvised explosive devices. The latest incident occurred on 25th April, when Lieutenant General Yaroslav Moskalik, a senior Russian military officer, was killed in a suburb east of Moscow when an improvised explosive device filled with shrapnel was concealed in a car parked near his home and detonated as he walked past. This attack is very similar to the one that took place in December 2024 in which Lt. Gen. Igor Kirillov, who served as the commander of the Russian Radiological, Chemical, and Biological Defence, was killed by an explosive device hidden inside an electric scooter, which was left next to the entrance of the building where Lt. Gen. Kirillov lived.

In another notable operation, a batch of FPV (First-Person View) drone goggles sent to Russian military units were rigged with explosives and delivered as part of 'humanitarian aid'. Russian military personnel noticed signs of tampering with the packages, leading to a further inspection and the discovery of concealed explosives. Each device contained about 10-15 grams of explosives, enough to kill or seriously injure a person.

Several rounds of indirect peace talks initiated by the newly elected US government, so far have not produced any tangible results due to the irreconcilable positions of the warring parties. At the time of writing, Kyiv and western leaders called for a 30-day pause in fighting. On 11th May, Moscow proposed to resume direct negotiations with Kyiv, which were interrupted in April 2022. It remains to be seen whether the talks (if they take place) will be able to bridge the differences between the two sides and lead to a de-escalation of the conflict.

Ireland

Explosive-laden drones have emerged as a significant security concern in Ireland[1], particularly in the context of organised crime and prison smuggling. In the latest development, Gardaí are currently investigating what appears to be an attempt to drop a pipe bomb from a drone on a house in north Dublin. The wreckage of the drone and an intact pipe bomb were found in the garden of a house in Glenties Park, Finglas, late on 4th May 2025 after it appeared to have crashed at the wrong address. Authorities are concerned that the gangland feud linked to the incident will now escalate sharply. These developments reflect a broader trend where criminal organizations are leveraging drone technology to carry out targeted attacks using explosives.

MIDDLE EAST

Israel–Gaza Conflict

In the Middle East, Israel remains mired in Gaza in its efforts to release the remaining hostages and defeat Hamas after its attacks on Israel in October 2023. There are conflicting reports of the number of hostages in the Hamas captivity. According to the latest statement of Israeli Prime Minister Benjamin Netanyahu there was "uncertainty" over the condition of three of the 24 hostages previously believed to be alive[2]. Amid continuation of the ongoing hostilities in the Gaza Strip there is a growing concern over the humanitarian situation and the presence of unexploded ordnance (UXO) which poses a serious threat to civilians and humanitarian aid efforts following intense military operations and bombardments. In addition, Gaza lacks sufficient mine clearance teams, access to modern demining technology and equipment, and the ongoing conflict makes it difficult to conduct surveys and explosives clearance operations.

Yemen crisis

Since Israel launched a military offensive against Hamas in the Gaza Strip following the Palestinian militant group's deadly attack on Israel on 7th October 2023, the Iran-backed Houthis in Yemen have stepped up their military actions, particularly targeting shipping in the Red Sea and Israeli mainland.

In an attempt to keep the vital Red Sea trade route open, the United States and Britain have responded with airstrikes against Houthi targets, while other countries independently patrol the waters near Yemen. The Israeli military has carried out several airstrikes against Houthi weapons facilities, command and control centres, and critical installations, including the port of Hodeida and Yemen's main airport in Sanaa. On 6th May 2025, a ceasefire agreement between the United States and the Houthis came into effect, ending the US and UK airstrikes. The Houthis agreed to stop their attacks on shipping in the Red Sea, however they stressed that the ceasefire does not apply to Israel "in any way, shape or form." It remains to be seen whether the US-Houthi ceasefire will hold or whether Israel can force the Houthis to stop their attacks through sustained military and diplomatic efforts.

1 https://www.irishtimes.com/crime-law/2025/05/07/drone-pipe-bomb-incident-raises-concerns-of-serious-feud-escalation/
2 https://www.bbc.co.uk/news/articles/c8d1pngdjzmo

Turkey

On 1st May 2025, the Kurdistan Workers' Party (PKK) declared a ceasefire after 40 years of conflict with Turkey that have killed tens of thousands of people. The PKK, which is designated a terrorist group by the United States, the European Union and Turkey, called on Ankara to release its leader Abdullah Ocalan, who has been jailed since 1999. On 12th May 2025, in a historic move, the PKK announced its plan to disband and disarm, potentially ending four decades of conflict with Turkey. The last significant attack attributed to the PKK occurred on 23rd October 2024, when they targeted the Turkish Aerospace Industries (TAI) headquarters near Ankara. The attack left five people dead and 22 wounded.

Post-Assad Syria

Syria is currently divided among several armed groups and regional powers. Hayat Tahrir al-Sham (HTS) controls much of the western and central parts of the country, including Damascus, and has initiated efforts to unify armed factions under a national defence framework. The Syrian Democratic Forces (SDF), a Kurdish-led alliance, maintains control over north-eastern Syria but has faced pressure from Turkish-backed Syrian National Army (SNA) forces, leading to ongoing clashes in areas like Tal Rifaat and Manbij. The Islamic State (ISIS) has exploited the power vacuum carrying out around 700 attacks in 2024. ISIS has also attempted to incite sectarian violence, including plans to target Shia holy sites, which were thwarted by HTS forces. A series of mass killings and massacres against Alawites occurred in Syria from 6th to 17th March 2025, with a resurgence in early April. Over several days of the sustained attacks in the coastal area of the country in Tartus, Latakia and Hama governorates, armed groups killed entire families, including women and children[3]. The UN High Commissioner for Human Rights (OHCR) spokesperson Thameen Al-Kheetan said the agency had documented at least 111 killings, though the true

3 https://edition.cnn.com/2025/03/12/middleeast/syria-sectarian-violence-un-ohcr-intl-hnk/index.html

number is believed to be far higher. According to a war monitor, the bloodshed saw more than 800 people killed in clashes between armed groups loyal to Bashar al-Assad and forces loyal to the new Syrian regime.

Mine clearance in Syria remains a critical and urgent humanitarian challenge in 2025, as the country continues to grapple with the legacy of its 14-year civil war. International organizations, including The HALO Trust and UNMAS, have intensified their efforts to address the contamination. UNMAS has surveyed over 83 million sq. m and removed 1,102 explosive ordnance items between August 2023 and January 2025, focusing on high-priority areas such as Rural Damascus, Aleppo, and Latakia. Despite these efforts, challenges persist, including limited funding, bureaucratic obstacles, and the vast scale of contamination. The Syrian Network for Human Rights (SNHR) has documented at least 3,521 civilian deaths due to landmine explosions since 2011.

SOUTH ASIA

India–Pakistan Conflict in Kashmir

The India–Pakistan conflict in Kashmir is one of the longest-running territorial disputes in modern history, rooted in the partition of British India in 1947. Indian-administered Kashmir has seen a decades-long insurgency which has claimed thousands of lives.

In late April 2025, tensions between India and Pakistan escalated dramatically following a militant attack in Indian-administered Kashmir that killed 28 civilians, mostly Hindu tourists. India attributed the attack to Pakistan-based militants, which Pakistan denies, and responded with missile strikes against militant groups it claims are backed by Pakistan. In response, Pakistan fired multiple missiles and launched over 50 drones towards Jammu and Kashmir, Punjab and Rajasthan. The United States led efforts to de-escalate the conflict, resulting in India and Pakistan to agree to a ceasefire, but the risk of further escalation remains high, as the countries have accused each other of violations shortly after the agreement came into force.

Jaffar Express attack in Pakistan

On 11th March 2025, the Balochistan Liberation Army (BLA) attacked the Jaffar Express, a Pakistani passenger train traveling through the Bolan Pass in Balochistan, taking around 440 passengers hostage, including a significant number of women and children. The attackers, who were reportedly in touch with their foreign handlers in Afghanistan via satellite phone, detonated explosives in tunnels and on the train tracks before opening fire on the train, halting it in a mountainous area difficult for authorities to reach. The terrorist organization had issued a 48-hour ultimatum to release the Baloch political prisoners, threatening to execute the hostages, although they had already released some of them. Within 30 hours, security forces killed all 33 militants, including the suicide bombers, and rescued 354 hostages. The operation left at least 64 people dead, including 18 soldiers and 33 attackers, and wounded 38. The BLA claimed to have killed 50 security personnel and 214 hostages, although those figures were disputed by Pakistani officials. The hijacking took place against the backdrop of almost daily IED and gun attacks on the security personnel and civilians in Balochistan and Khyber Pakhtunkhwa provinces.

AFRICA

Sahel & Lake Chad basin

The Sahel continues to be a hotspot for extremist activity, accounting for over half of all militant Islamist incidents on the continent. Groups like Jama'at Nusrat al-Islam wal-Muslimin (JNIM) and the Islamic State in the Greater Sahara (ISGS) have intensified attacks, leading to nearly 11,000 fatalities in 2024 alone. Since 2010, over 1,600 IED-related incidents have been recorded across the region, resulting in at least 6,680 deaths and more than 9,000 injuries. These devices have been used to target security forces, UN peacekeepers, and civilians, particularly in countries like Mali, Burkina Faso, and Niger. The proliferation of IEDs has also led to environmental contamination and significant economic losses, impeding development efforts and displacing millions. Inadequate border controls and regulatory frameworks allow for the

unchecked movement of IED components and the establishment of manufacturing networks. In the Lake Chad basin women play a significant role in trafficking important components and bomb-making materials through checkpoints and across borders because they are rarely subjected to body searches[4]. The Boko Haram, typically known for its conservative views on women's social status, has permitted women greater mobility because they are aware women are usually above suspicion with law enforcement authorities. Women often conceal IED components in various ways, such as strapping them to their backs disguised as 'babies', hiding them in four-litre bottles or concealing components under pillows. Once past checkpoints, women either deliver the components directly to remote Boko Haram hideouts or drop the products off at pre-designated locations, in the bush or on farms, creating additional challenges for law enforcement and counterterrorism efforts in the region.

Nigeria

In 2024, Nigeria experienced 197 attacks from improved explosive devices (IEDs) – an average of nearly one IED attack every two days. On 8th May, an IED explosion in Mafa Local Government Area of Borno State, left five children injured, one of whom lost a hand. The explosion occurred when the children unknowingly tampered with an IED device. On 28th April at least 26 people, including women and children, were killed when vehicles detonated by IEDs planted in Nigeria's north-eastern Borno State. The victims were travelling in vehicles along the road from Rann to Gamboru Ngala, where Boko Haram terrorists planted a number of explosive devices. In addition to the 26 fatalities, three people sustained serious injuries.

The Nigerian National Security Adviser (NSA), Mallam Nuhu Ribadu, has called for development of effective mechanisms[5] to enhance the ability to prevent and counter the use of IEDs by terrorist groups in West Africa. Ribadu said that the threat of terrorism knows no bounds, adding that it was through collaborative efforts by critical stakeholders that they could effectively confront and defeat the menace.

On 25th March Cameroonian troops stationed in Wulgo, Nigeria, have been killed in the jihadists' attack. According to AFP, the attackers used rocket-propelled grenades and 'armed drones' to inflict heavy casualties. The attack, one of the region's deadliest incidents in recent months, comes as armed groups in west Africa pivot towards the use of cheap, recreational drones modified into one-way, explosives-laden attack vehicles. Armed groups in Nigeria and the Sahel have long used drones for surveillance and filming propaganda, however, a shift is under way as jihadists and separatists outfit them for attacks. Jihadist groups in Mali and Burkina Faso have claimed to use drones equipped to drop grenades from above, as well as explosive-laden 'suicide drones' that crash into targets[6].

DEMINING EFFORTS

Bosnia and Herzegovina

According to the recent reports, the Armed Forces of Bosnia and Herzegovina (BiH) cleared 903,326 square meters of land in 2024 as part of ongoing demining efforts[7]. In total, over 14.7 million square meters of land were returned to civilian use, contributing to the development and safety of local communities. Despite operational challenges, the Armed Forces successfully implemented 61.28 percent of the national mine action plan. Demining activities took place across 18 municipalities, including 13 in the Federation of BiH and 5 in Republika Srpska.

Vietnam

Marking another step in the US and Vietnam's decades-long effort to heal the scars of war, a new training range for explosive ordnance disposal (EOD) has recently been inaugurated in Hanoi's outlying district of Ba Vi. The facility was funded by the Office of

4 https://enactafrica.org/enact-observer/under-the-radar-women-traffic-ied-parts-to-boko-haram
5 https://nannews.ng/2025/05/06/nsa-seeks-effective-mechanism-to-tackle-ieds-usage-by-terrorists/
6 https://www.msn.com/en-us/news/world/nigeria-sahel-militants-embrace-diy-drone-warfare/ar-AA1BLzq6
7 https://english.news.cn/europe/20250424/e84b9d702e2f414fbd81ec940c36992e/c.html

Defence Cooperation (ODC) under the US Embassy in Vietnam and delivered to the Vietnam National Mine Action Centre (VNMAC), as part of Vietnam's National Mine Action Programme for the 2010–2025 period, which seeks to address the deadly legacy of unexploded bombs and mines left from the war. The two-hectare range broke ground in July 2024, supported by a grant of over 700,000 USD from the US Government[8].

Cambodia

According to a report from the Cambodian Mine Action and Victim Assistance Authority (CMAA) released at the end of April 2025 the number of people injured or killed by landmines dropped by 26% in the first four months of this year[9]. In another positive development, on 29th April the Koh Kong's Botum Sakor district was officially declared mine-free[10], benefiting about 100,000 residents, through grant aid from the Indian government. Ly Thuch, first vice president of the Cambodian Mine Action and Victim Assistance Authority, expressed appreciation for India's support in helping the government address the dangers posed by landmines and explosive remnants of war. However, it was also reported that nearly half of all mine accidents in Cambodia over the past decade have occurred outside of officially identified minefields - an alarming indicator that vast areas remain unsurveyed.

IN THIS EDITION

In his comprehensive paper "Infrastructure and commercial projects: EO clearance and risk management," Dr Robert Keeley of RK Consulting (EOD) Ltd outlines the differences between humanitarian and commercial perspectives of mine action and how they influence the attitude to EO clearance in commercial projects and infrastructure. He begins by describing the UN guiding principles of Neutrality, Humanity, Impartiality, and Independence. Under the 1997 APMBC and 2008 CCM conventions there is a requirement for humanitarian mine action to clear all EO contamination within a prescribed area, whereas in commercial projects the requirement is to clear EO specifically relevant to the project in hand. He provides a formal definition of risk, attitudes to risk and potential consequences – physical risk, project risk and reputational risk. In commercial mine action EO clearance is seen as an enabler to allow the wider goals of the project to be achieved. He describes the overall risk management process and provides a detailed table on recommended risk management/treatment approaches for the clearance of commercial project sites. He provides a most useful SPR table to assist in the identification of an appropriate mine action intervention – 'S' being the Source of the potential hazard, 'P' is the Pathway - the route to the potential hazard and 'R' is the Receptor – for example a person or a building benefitting from the clearance. He also identifies possible responses to the hazard.

In his technically detailed article Lieutenant Commander Murat Aydoğmuş of the Turkish Navy and based at the NATO C-IED Centre of Excellence, examines the impact of AI on underwater detection and identification of IEDs on or buried in the seabed. He points out that the increasing reliance on naval and offshore assets for trade, energy production and defence means that the underwater threat has become a critical concern for global security. He describes how AI has revolutionised underwater threat detection. He outlines technical approaches to threat detection such as sonar scanning, magnetic anomaly detection, diver inspection and ROVs. He describes the operations of two sonar systems, the Side Scan Sonar (SSS) and Synthetic Aperture Sonar (SAS). Both systems produce detailed imagery of the underwater environment. The SSS is a towed system and emits soundwaves which interact with the sea floor and objects on it or buried in it, producing an acoustic reflection. The SAS is mounted on a UUV and monitors and records back scattered signals from the seabed. It produces a finer resolution than the SSS system. Magnetic anomaly detection uses

8 https://vietnamnet.vn/en/vn-us-boost-ties-with-new-uxo-disposal-training-site-launch-2398876.html
9 https://www.khmertimeskh.com/501675501/cmaa-reports-26-drop-in-mine-blast-victims-in-first-quarter-of-year/
10 https://www.khmertimeskh.com/501674937/botum-sakor-district-in-koh-kong-to-be-declared-mine-free

a sensitive magnetometer to detect disturbances in the Earth's magnetic field. For underwater detection purposes it may be attached to ships, UUVs or aircraft. The integration of Artificial Intelligence into underwater detection systems enhances situational awareness, efficiency, and decision-making capabilities.

In a widely researched article Lt Col Jose M Rufas of the NATO C-IED Centre of Excellence states that despite intense efforts by national and international authorities, the internet remains the most prolific source of technical knowledge for the planning and preparation of terrorist attacks during this century to date. It provides extensive online dissemination of manuals, videos, and instructions on the manufacture of HME and IEDs. Jihadists and other terrorists and extremists can source a wealth of content describing the planning of attacks, acquiring precursors and components, the manufacture of explosives and the construction of devices. The current conflict in Ukraine has witnessed a significant uptick in this type of online information provided by supporters of both sides of the conflict. To date this year the media offices of DAESH/ISIS have portrayed an increasing number of explosives related threats in their propaganda posters. A worrying trend during 2024 and 2025 has been the increasing diversity and locations of sources in addition to the traditional Arabic and English languages information. It is now possible to find information in the Brazilian, German, Italian, Russian, Spanish, and Turkish languages. A further concern has been the reappearance of hitherto dormant sources of terrorist information including, inter alia, the DAESH related "Al Saqri Foundation for Military Science" that is once again producing a wealth of terrorist related information. It is assessed that the ongoing conflict campaign in Ukraine will continue to be a valuable source of reference for IED manufacture and deployment.

In his informative article Wilder Alejandro Sanchez, an international defence and security analyst, reviews the current state of landmine removal in post-conflict Azerbaijan. The Azerbaijani government is currently undertaking extensive clearance of landmines, UXO and other ERW resulting from the 2020 and 2023 conflicts between Armenia and Azerbaijan in order to return the contaminated territories to civilian and commercial use. The contamination comprises both AP and AV landmines and other UXO and ERW. The Mine Action Agency of the Republic of Azerbaijan is tasked with the extensive clearance operations and has made good progress to date, but much more needs to be done. Civilians returning to the territory remain in peril and from 2020 to 31st December 2024 there were 229 landmine explosions in Karabakh resulting in 382 victims and 70 fatalities. Azerbaijan will require continuing international assistance to decontaminate Karabakh territory. To date the US, UK, EU, Canada, Japan, Turkey, UNHCR, UNDP and ICRC have provided assistance and GICHD has provided substantial technical assistance including IMSMA. A positive development has been the involvement of female demining teams in the clearance activities. The decontamination of the Karabakh region will remain a long-term project. ■

Rob Hyde-Bales biography

During his career in the UK Royal Engineers, **Rob Hyde-Bales** was responsible for landmine clearance in Libya and, more latterly, Afghanistan in the running of the first United Nations humanitarian landmine clearance training programme – Operation Salam. The programme trained Afghan male refugees in landmine clearance techniques, and Afghan women and children in mine awareness and avoidance training. More recently he set up the Caribbean Search Centre in Kingston, Jamaica. The Centre is designed to train security forces across the Caribbean in modern search techniques. After retiring from the army he joined Cranfield University at Shrivenham, near Oxford, and undertook a research project on behalf of the UK Ministry of Defence that examined ways to improve the sharing of IED threat information between the military and civilian organisations in hazardous areas.

THE ONLY CONFERENCE BRINGING TOGETHER MILITARY, HUMANITARIAN GROUPS, AND INDUSTRY LEADERS TO DISCUSS AND IMPROVE OPERATIONS IN EOD AND DEMINING

Defence iQ

COUNTERING EXPLOSIVE THREAT & DEMINING

23 - 24 SEPTEMBER, 2025
COPTHORNE TARA HOTEL, LONDON, UK

ADVANCING EOD AND C-IED CAPABILITIES: COOPERATION, INNOVATION, AND CAPACITY BUILDING

"THE DIFFERENT PERSPECTIVES ACROSS MILITARY AND NGOS WERE STIMULATING AND GOOD TO SEE NEW INDUSTRIAL DEVELOPMENTS"
SENIOR RESEARCHER, DSTL

VIEW THE AGENDA HERE

LEADING SPEAKERS FROM ACROSS THE EOD AND DEMINING SECTOR:

Colonel Darren Fisher,
Commander,
29 EOD & Search Regiment

Stephen Ingram,
Global Technical Advisor HMA,
Mine Advisory Group

Brigadier General Jihad Al Bechelany,
Director,
Lebanese Mine Action Centre (LMAC)

Major Mark Fetters,
Counter-Explosive Ordnance,
Army Futures Directorate

Georgina Darlow,
Advisor in the Research and Innovation Programme,
Geneva International Centre for Humanitarian Demining (GICHD)

+44 (0) 113 521 0042 enquire@defenceiq.com **defenceiq.com/events-counteringexplosives**

UNDERSTANDING AND THREAT ALIGNMENT WITHIN A C-IED ENTERPRISE

By Paul Amoroso, an explosive hazards specialist at Assessed Mitigation Options (AMO) consultancy.

INTRODUCTION

In previous articles published in The Counter-IED Report, the author has advocated for a whole-of-society approach[1] to countering the use or threatened use of IEDs through a national Counter-IED (C-IED) enterprise.[2] Such approaches necessitate a coordinated effort among stakeholders with complex institutional structures, requiring internal coherence and collaboration to ensure effective C-IED strategies. A clear and shared understanding of the IED threat is essential to effectively coordinate C-IED efforts,[3] align them with the specific threat, and optimise resources for both responding to and preventing their use. To be effective, any national C-IED enterprise must first fully understand the problem it aims to counter. This begins with recognizing the current IED threat and anticipating potential future threats. This understanding of the threat will guide the structure and composition of a C-IED enterprise, requiring a careful and strategic selection of stakeholders to ensure its effectiveness. It will also influence the enterprise's strategic goal along with the C-IED efforts invested in and their

1 A whole-of-society approach to C-IED is a comprehensive approach to C-IED involving a broad array of stakeholders contributing to a C-IED enterprise. It can include multiple elements of state security, defence, government departments, ministries, offices, and agencies along with civil society organisations, commercial and industry entities as well as international and regional organizations. Whole-of-society C-IED approaches often have stakeholders with complex institutional structures and procedures requiring internal coherence, a cooperative and collaborative culture between members to support effective C-IED efforts through a shared understanding of the IED threat faced. Source: Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25.

2 A C-IED enterprise refers to the collective efforts aimed at countering IED threats. It can involve anything which is intended to predict, discover or detect, prevent, protect against, respond to or neutralise, recover from or exploit, mitigate against, or deter IED attacks.

3 C-IED efforts may be responsive, preventative or cross-cutting in nature. Such efforts include, inter alia, legal instruments, training, mentoring, advice, operational and tactical or technical assistance, technology and equipment provision, intelligence activities, investigations and actions against an IED system, interagency and international cooperation, control of explosives and other IED components as well as any other investment made to respond to and ultimately prevent IED use. Source: Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25.

objectives. Key entities central to understanding in a C-IED enterprise can include the national lead entity for C-IED, the Office of the National Security Advisor, and various security services.[4] The importance of a designated lead entity[5] has previously[6] been emphasized. It is important to remember no one-size-fits-all and the best fit to lead any national C-IED enterprise will involve consideration of the context, limitations imposed, and importantly the threat.[7] The lead entity must monitor and adapt C-IED efforts to the evolving threat landscape.

Understanding is a critical cross-cutting element within any C-IED enterprise and one which has two aspects to it. One is understanding the threat and second is understanding the effectiveness of the C-IED efforts invested in. This article will explore the concept of understanding within a C-IED enterprise and the importance of aligning C-IED efforts with the threat. We will begin by examining the significance of understanding within a C-IED enterprise, highlighting its critical role in the enterprise's success and the potential risks that arise from its absence. We will then examine the need for and ability to achieve initial and sustained understanding within the enterprise. The importance of a C-IED enterprise remaining threat aligned is shown by examining its importance when personnel need to operate in a high threat IED environment. The evolution of the IED threat has an impact across all elements of the enterprise, which will be illustrated by examining its importance regarding IED component control and C-IED border controls. This is the first in a series of articles examining how to develop and sustain an accurate IED threat picture to optimize understanding and ensure the C-IED efforts invested in remain effective as threats evolve.

UNDERSTANDING WITHIN A C-IED ENTERPRISE

A previous article in The Counter IED Report stated that 'before you counter a problem, you need to know the problem.' In the case of C-IED this refers to understanding the use or threatened use of IEDs, so that in time effective and efficient C-IED efforts may be invested in as part of a C-IED enterprise to at least match but ideally overmatch the IED threat.'[8]

One of the fifteen previously[9] proposed elements to form the basis for any national C-IED enterprise, was understanding. Security centric C-IED frameworks often have understanding as the foundation upon which the lines of effort of attack the network, defeat the device, and train the force are built upon.[10] As such, understanding within a C-IED enterprise is critical to effectively responding to and ultimately preventing IED use. It can be a challenging element of an enterprise to get right, as it involves more than just having insightful comprehension of the IED threat. It also requires a thorough grasp of all elements of the enterprise to evaluate the effectiveness of all efforts invested in and the overall impact on countering the IED threat. In fact, "the key fundamental C-IED enabling action of 'understanding' both the problem and the C-IED efforts invested in, is deemed essential.'[11]

4 Source: Building the C-IED Enterprise to Counter the IED System, The Counter-IED Report, Winter 2023/24.

5 In a previous article of this publication, Colonel H R Naidu Gade, spoke of the need to designate what is called a nodal agency, "to coordinate and track progress across all the agencies at national, state, and local levels toward building the C-IED capabilities. It should facilitate harnessing the innovative potential of the research and development organizations to meet a dynamic, complex, and adaptive threat and to promote an informed and agile research and acquisitions process that stays ahead of the threat and develops timely and effective C-IED systems and solutions." Source: India – The National Counter-IED Strategy, The Counter-IED Report, Winter 2023/ 2024, by Colonel H R Naidu Gade (Retd), pp. 40.

6 Necessity of a Designated Lead Entity within National C-IED Enterprises, The Counter-IED Report, Spring/Summer 2024.

7 Necessity of a Designated Lead Entity within National C-IED Enterprises, The Counter-IED Report, Spring/Summer 2024.

8 Understanding and Maximising C-IED Information Sharing, The Counter-IED Report, Autumn 2023.

9 Building the C-IED Enterprise to Counter the IED System, The Counter-IED Report, Winter 2023/24.

10 These three lines of effort are captured within the fifteen elements, outlined in Building the C-IED Enterprise to Counter the IED System, The Counter-IED Report, Winter 2023/24.

11 A Strategic Principles Approach to Regional C-IED Enterprises, The Counter IED Report, Spring/Summer 2023.

'The criticality of understanding in support of any coherent C-IED enterprise is both cross-cutting and multi-dimensional, referring to the need to comprehend inter alia:

- Why and how IEDs are used;
- Use of appropriate terminology;
- What a national C-IED enterprise entails;
- Maintaining an accurate IED threat picture for effective C-IED decision making;
- Role and importance of exploitation in maintaining an accurate IED threat picture;
- Timely information sharing between C-IED stakeholders;
- Appropriate classification of C-IED information.'[12]

It requires both an initial assessment of the threat and a baseline assessment of existing C-IED elements which can then be used to inform the design and development of a C-IED enterprise. It subsequently requires on-going threat assessment to ensure the C-IED efforts invested in remain threat aligned along with an embedded monitoring, evaluation, and learning (MEL)[13] process to inform an understanding of the effectiveness of the C-IED elements invested in. As such, a system to maximise initial and on-going understanding needs to be developed through initial baseline assessments, on-going threat assessment and embedding a MEL process within the enterprise. With a thorough understanding of the threat as well as all of its elements, an enterprise is best positioned to remain threat aligned, effective, and efficient over time.

Evolution of Threat and Effectiveness of C-IED Efforts Invested In

Another article discussing the management of a C-IED enterprise, outlines the need for C-IED activities to be synchronized and unity of effort to be achieved across its constituent C-IED efforts. It stated 'the temptation to pursue neat and clean synchronisation across C-IED efforts should be avoided, especially that which is rigid and inflexible. There is often a need to simultaneously invest in various C-IED efforts, each with different priorities. Over time, these initial prioritisation requirements will change, necessitating adaptation and further synchronisation. Thus, flexibility is required as the rate at which various C-IED efforts mature to being impactful can vary, the threat can evolve, and the wider security environment can change.'[14] This evolution of the IED threat, variation in the effectiveness of C-IED efforts, and changes in the broader security landscape indicate that although an accurate understanding may be achieved during the design and development of an enterprise, this understanding will inevitably need to adapt over time. Therefore, there is a need for both initial and sustained understanding to support a C-IED enterprise.

The Risk Posed by a Lack of Understanding

Employing strategic principles in support of a regionally coherent C-IED enterprise has previously been proposed.[15] Several approaches were considered in developing an analysis framework to facilitate the identification of such principles. Through the examination and combination of four such approaches[16] a seven-question framework[17]

12 Understanding and Maximising C-IED Information Sharing, The Counter-IED Report, Autumn 2023.

13 'Monitoring and evaluation within a C-IED enterprise involves observation and documentation of the C-IED efforts invested in, followed by the subsequent evaluation of their impact on the IED threat. This process of observation and analysis is intended to identify lessons for each of the C-IED efforts invested in.' Source: Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25 edition.

14 Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25 edition.

15 A Strategic Principles Approach to Regional C-IED Enterprises, The Counter-IED Report, Spring/Summer 2023.

16 These four approaches involved identifying ends, ways and means; considering the situation, task, execution, authority, and support demands; examining what, why, who, where, when and how (5W+H) of the problem; and a generic set of seven questions which may be applied to any planning scenario which is adapted from the military seven question estimate.

was developed to identify optimal C-IED strategic principles for a given IED affected state or region,[18] to achieve the required impacts and outcomes from C-IED donor assistance.[19] This seven-question framework can equally be applied as a methodology to establish what C-IED efforts need to be invested in by a national enterprise. With the problem statement known,[20] the seven question framework[21] poses the following questions in terms of countering the use and threatened use of IEDs.

1. What end-state is desired
2. What actions are to be taken?
3. Who are to take the actions?
4. When are the actions to be taken?
5. Where are the actions to be taken?
6. What risks need to be managed?
7. What resources do the actions require?

The question of 'what risks need to be managed' has two aspects to it; namely, what will optimize the likelihood of success of a national C-IED enterprise and secondly what risks need to be mitigated against. Five recurrent risks were identified with the first[22] being a lack of understanding within the C-IED enterprise. As such, not only is understanding essential for a C-IED enterprise to be effective, but a lack of understanding also poses a risk to it being effective and ultimately a success but also often leads to a waste of often valuable resources.

The risk arising from a lack of understanding can be minimized through four key steps: conducting an initial threat assessment, establishing a baseline evaluation of existing C-IED efforts, maintaining ongoing threat assessments, and integrating a structured MEL process into the C-IED enterprise. As such, understanding within the C-IED enterprise occurs at two critical junctures: initially and on an ongoing basis to sustain an accurate understanding. When this is done the C-IED efforts invested in can remain threat aligned, and their effectiveness can be monitored and adjusted as required when needed.

17 The seven-question framework presented previously uses seven questions to establish what C-IED strategic principles best suit a given IED affected region to achieve the required impacts and outcomes from C-IED donor assistance; however, it can equally be applied as methodology to establish what C-IED efforts need to be invested in by a national C-IED enterprise.

18 Such principles can serve as the foundation for reasoning and decision-making about how IED affected states, their regional organisations, and international organisations providing C-IED donor assistance can respond strategically to the threat posed by IEDs. The desired end state for such principles is that they support the development of coherent C-IED enterprises to at least match, but ideally overmatch, the threat posed by IEDs. Source: C-IED Strategic Principles for East Africa, The Counter-IED Report, Autumn 2023.

19 C-IED donor assistance refers to C-IED support provided on a bilateral basis, on a joint initiative from two or more States or by an international organisation, e.g., EU, League of Arab States, ECOWAS etc or an alliance e.g. NATO, to an IED affected state or region. Source: Is Implementation of Western C-IED Enterprises Suitable When Providing Donor C-IED Assistance, The Counter-IED Report, Spring/Summer 2023; C-IED Strategic Principles for East Africa, The Counter-IED Report, Autumn 2023; Necessity of a Designated Lead Entity within National C-IED Enterprises, The Counter-IED Report, Spring/Summer 2024.

20 In the development of the seven-question framework the starting point was consideration of 'what is the situation and how does it affect us?' This provides the problem statement being addressed. In this case, we have the starting assumption that an IED threat exists in a given region, state or locality requiring an IED affected state or number of states to engage in a C-IED enterprise. As this problem statement is known, no such question needs to be included in the analysis.

21 This framework uses seven questions to establish what C-IED strategic principles best suit a given IED affected region to achieve the required impacts and outcomes from C-IED donor assistance.

22 Others included, lack of coherence, coordination and cooperation often leading to unnecessary competition and waste of resources amongst stakeholders; lack of power of enforcement to compel stakeholders to engage effectively in the C-IED enterprise; and finally, the risk of some C-IED efforts having negative counterproductive effects which overall damage the C-IED enterprise.

INITIAL UNDERSTANDING

During the design and development of a C-IED enterprise, it is necessary to undertake an initial IED threat assessment as well as a baseline assessment[23] of the maturity or lack thereof, of existing C-IED efforts being invested in.

Initially Assessing the IED Threat

It is essential to have a clear understanding of the IED threat when designing and developing a C-IED enterprise, to ensure that the enterprise is aligned with the specific threat from the beginning. The methodology adopted or adapted for this initial IED threat assessment is the focus of a series of articles throughout 2025.

Assessing Existing C-IED Capabilities

Initial 'understanding is informed by a baseline assessment, which compares current C-IED capabilities to those required to achieve the planned C-IED enterprise.'[24] Such a baseline assessment can determine 'the maturity or lack thereof, of the key elements which contribute to a C-IED enterprise.'[25] The seven-questions framework can be adapted to determine the most effective C-IED efforts for the enterprise to invest in. These efforts can then be evaluated against current efforts to identify the necessary level of investment to achieve the desired outcomes. This process may also highlight new C-IED efforts that require investment. A more common approach to undertaking a national C-IED baseline assessment is to use the UNIDIR C-IED CMM self-assessment tool[26] or adaptations of this.

SUSTAINED UNDERSTANDING

Once the findings of the initial threat assessment and baseline assessment are assimilated into a C-IED enterprise, the most appropriate C-IED efforts can be invested in and prioritized as part of a broader strategic plan. Once operationalized, the C-IED enterprise needs to be managed with the objectives of remaining threat aligned, effective and efficient, which 'collectively present a challenge to typical linear, rigid management practices, necessitating the need for flexibility.'[27] A flexible C-IED enterprise is one that is agile[28] that can effectively respond to and ultimately prevent IED incidents. One of the 15 elements proposed as the basis for a C-IED enterprise is adapting C-IED efforts. Adaptation of the enterprise is necessary owing to the evolution of the threat and changes in the effectiveness of the C-IED efforts invested in. To support such adaptation, there is a need for internal mechanisms to monitor, evaluate and feedback lessons identified into the enterprise in relation to both the IED threat as it evolves as well as the effectiveness of the C-IED efforts invested in.

Evaluating Effectiveness and Adaptation

Integrating a Monitoring, Evaluation, and Learning (MEL) process within the C-IED enterprise serves as a tool to assess and improve the effectiveness of C-IED efforts. It enables the identification of lessons that guide necessary adaptations to enhance impact. Additionally, the MEL process strengthens oversight by tracking the progress of C-IED initiatives, ensuring they remain aligned with objectives or highlighting areas requiring adjustment. This, in turn, can contribute to a more efficient C-IED enterprise by optimizing the use

23 Phases within a C-IED Enterprise, The Counter-IED Report, Autumn 2024.

24 Building the C-IED Enterprise to Counter the IED System, The Counter-IED Report, Winter 2023/24.

25 A Conceptual Framework for C-IED Enterprise Design, The Counter-IED Report, Autumn 2024.

26 https://unidir.org/publication/counter-ied-capability-maturity-model-and-self-assessment-tool/

27 Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25.

28 This need for agile C-IED responses is discussed in 'Agile C-IED Enterprises', The Counter-IED Report, Winter 2024/25.

of invested resources. As monitoring and evaluation of the effectiveness of C-IED efforts can identify lessons, informed decisions to 'modify existing or invest in new C-IED efforts,'[29] are empowered. Once 'political backing to modify the enterprise'[30] is secured, 'an efficient process, involving key stakeholder engagement, resource mobilization[31] and communication, is needed to ensure the resulting constituent C-IED efforts within the enterprise remain threat aligned, effective and efficient.'[32] As such, embedding a MEL process into a C-IED enterprise is a key tool to achieving an agile enterprise.

Maintaining Awareness of Evolving IED Threats

While the effectiveness of the C-IED efforts invested in will be determined by a number of factors,[33] the IED threat will be the primary one. Parallel to an embedded lessons learned process; threat monitoring needs to be on-going to detect changes in IED use and horizon scan.

'An IED threat is normally an evolving and dynamic problem'[34] as the threat being confronted will evolve over time in terms of the technical complexity and tactical sophistication as the IED network employing them will seek to circumvent the C-IED efforts invested against them. For this reason, it is important to acknowledge an IED threat typically evolves due to the action-reaction-counteraction cycle that plays out between IED threat actors and those engaged in a C-IED enterprise. Whatever approach is taken by a national C-IED enterprise, the fact that the threat will inevitably evolve due to the action-reaction-counteraction cycle, the C-IED efforts invested in need to remain agile.

The requirement for C-IED efforts to be agile, implicitly requires the C-IED enterprise to monitor their effectiveness and evaluate them to ensure they remain threat aligned.[35] Monitoring and evaluation of the effectiveness of the C-IED efforts invested in can detect IED threat evolution;[36] however, the primary means by which IED threat evolution can be detected is by dedicated efforts to maintain awareness of likely evolution in the IED threat. This requires ongoing monitoring of the IED threat, enabling timely adjustments to keep the enterprise threat aligned and agile.

Threat monitoring is intended to detect both threat evolution as well as horizon scan for emerging threats.[37] Timely C-IED intelligence products are the outputs from effective threat monitoring. These C-IED intelligence products should ideally provide feedback, through a collaborative information sharing culture, to the stakeholder community involved to ensure the efforts invested in and their respective prioritization remain threat aligned.

This stakeholder community can then use the information provided by such intelligence products, to update or change the IED threat picture, so that it remains threat aligned. By having within a C-IED

29 Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25 edition.

30 Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25 edition.

31 Resource investment will need to be considered over the medium to long term as the various efforts invested in will need to be maintained and probably modified as the IED threat evolves and the C-IED enterprise needs to be adapted, so that its stays threat aligned and continues to invest in the most appropriate ways under the legal framework it is required to operate. Source: Necessity of a Designated Lead Entity within National C-IED Enterprises, The Counter-IED Report, Spring/Summer 2024.

32 Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25.

33 These factors included 'the rate at which various C-IED efforts mature to being impactful can vary, the threat can evolve, and the wider security environment can change.' Source: Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25.

34 Understanding and Maximising C-IED Information Sharing, The Counter-IED Report, Autumn 2023.

35 A Conceptual Framework for C-IED Enterprise Design, The Counter-IED Report, Autumn 2024.

36 A Conceptual Framework for C-IED Enterprise Design, The Counter-IED Report, Autumn 2024.

37 Source: Regulating control of threat explosive precursor chemicals for use in improvised explosives, Background paper, Prepared by Paul Amoroso and Manon Blancafort for the Small Arms Survey, 20th January 2025.

enterprise an embedded MEL process, as well as an effective threat monitoring system, informed decisions, effective responses, and ultimately preventative measures, can be invested in and, when necessary, adjusted.[38]

THREAT ALIGNMENT IN HIGH THREAT IED ENVIRONMENTS

The need for timely and threat aligned C-IED capabilities are essential when 'security force and defence force personnel are required to operate in a high threat IED environment.'[39] These personnel 'will need to be provided with suitable threat aligned IED awareness and training which may be considered specialised preparation and can include the provision of certain specialised C-IED equipment. Examples of this include intermediate search capabilities such as route search, the use of electronic countermeasures (ECM) equipment or what may be considered level 1 exploitation. The aim of C-IED specialist preparation is to appropriately train and equip all those required to undertake key activities within any national C-IED enterprise. Such key C-IED activities include, inter alia, information management and threat picture development as part of understanding efforts as well as defeat the device activities, and exploitation activities.'[40]

THREAT ALIGNMENT OF IED COMPONENT CONTROL AND C-IED BORDER CONTROLS

Two of the preventative C-IED elements previously outlined are IED component control and border controls. Both need to be threat aligned at all times to be effective and are closely related in many of the C-IED efforts they support. IED component control involves developing and implementing measures to regulate and control access to IED components. These control measures may target explosive precursor chemicals deemed a threat due to their assessed risk of being used in the manufacture of improvised explosives. They may also be used to control access to switches identified as components in IEDs. Any state security entity with a role in identifying such chemicals or components, developing appropriate control measures, their implementation and enforcement will need to be involved in this element of a national enterprise.

Police or other law enforcement agencies may have primary responsibility for investigating and enforcing such controls domestically. It may also involve, border management authorities, particularly those with customs responsibilities required to monitor and enforce regulations related to the international movement of certain controlled IED components into or from the state. Wider border security entities may also be required to be on the lookout for and trained to identify the illicit movement of IEDs, components thereof as well as IED network personnel. They may also be trained and equipped to take appropriate safe action upon discovery of any suspected items or personnel. As such, border control is a key element in any national C-IED enterprise.

On-going monitoring of the chemicals and components in use in IEDs will be necessary to ensure evolution in the threat is detected. Subsequent appropriate adjustment in the required regulation and control measures will need to be put in place. These adjustments will then need to be communicated to those who need to implement and enforce them, which may also entail training in new procedures or associated equipment.

38 Source: Regulating control of threat explosive precursor chemicals for use in improvised explosives, Background paper, Prepared by Paul Amoroso and Manon Blancafort for the Small Arms Survey, 20th January 2025.

39 Nesting C-IED Appropriately Within a State's National Security Architecture, The Counter-IED Report, Spring/Summer 2024.

40 Nesting C-IED Appropriately Within a State's National Security Architecture, The Counter-IED Report, Spring/Summer 2024.

CONCLUSION

Understanding is a vital cross-cutting element of any C-IED enterprise, encompassing two key aspects: the threat itself and the effectiveness of the C-IED efforts invested in. To achieve effective understanding, it must be initially established during the design phase to guide the development of a national C-IED enterprise and subsequently sustained over time. Initial understanding requires an initial IED threat assessment as well as a baseline assessment of existing C-IED capabilities. Sustained understanding requires monitoring the evolving IED threat as well as assessing the effectiveness of C-IED efforts invested in. The importance of ensuring all C-IED efforts remain threat-aligned and efficient has been emphasized, with their efficiency depending on maintaining this alignment. However, as an IED system evolves to circumvent the C-IED efforts invested in against it, the IED threat is constantly evolving making this a dynamic and challenging endeavour. Despite these challenges, the C-IED enterprise needs to adapt, to ensure 'firstly it remains threat aligned, secondly the C-IED efforts invested in are optimised to support the overarching strategic goal of the enterprise and thirdly, to work efficiently and effectively within the resources provided to the enterprise.'[41]

Such adaptation is only possible through an embedded MEL process to inform an understanding of the effectiveness of the C-IED efforts invested in. It also requires on-going threat monitoring to detect changes in the threat and horizon scan for emerging threats. The ability to systematically undertake an initial threat assessment and to threat monitor on an ongoing basis requires the development and sustainment of an IED threat picture. Subsequent articles over the course of 2025 will examine how to develop and sustain an accurate IED threat picture to optimize understanding and ensure the C-IED efforts invested in remain effective as threats evolve.■

ABOUT THE AUTHOR

Paul Amoroso is an explosive hazards specialist and has extensive experience as an IED Threat Mitigation Policy Advisor working in East and West Africa. He served in the Irish Army as an IED Disposal and CBRNe officer, up to MNT level, and has extensive tactical, operational, and strategic experience in Peacekeeping Operations in Africa and the Middle East. He has experience in the development of doctrine and policy and was one of the key contributors to the United Nations Improvised Explosive Device Disposal Standards and the United Nations Explosive Ordnance Disposal Military Unit Manual. He works at present in the MENA region on SALW control as well as in wider Africa advising on national and regional C-IED strategies. He has a MSc in Explosive Ordnance Engineering and an MA in Strategic Studies. He runs a consultancy, Assessed Mitigation Options (AMO), which provides advice, support, and training delivery in EOD, C-IED, WAM as well as Personal Security Awareness Training (PSAT) and Hostile Environment Awareness Training (HEAT). This article reflects his own views and not necessarily those of any organisation he has worked for or with in developing these ideas.

LinkedIn profile: https://www.linkedin.com/in/paul-amoroso-msc-ma-miexpe-60a63a42/

41 Managing a C-IED Enterprise, The Counter-IED Report, Winter 2024/25.

IED CLASSIFICATION – BREAKING DOWN BOMB ATTACKS

By Paul Amoroso, an explosive hazards specialist at Assessed Mitigation Options (AMO) consultancy.

INTRODUCTION

This is the second article in a series examining how to develop and sustain an accurate IED threat picture to optimize understanding and ensure the C-IED efforts invested in remain effective as threats evolve. The first article titled, 'Understanding and Threat Alignment Within a C-IED Enterprise' emphasised understanding as a vital cross-cutting element of any C-IED enterprise, encompassing two key aspects: the threat itself and the effectiveness of the C-IED efforts invested in. The rest of this series of articles will focus on understanding the threat of IED attacks, through an IED threat picture.

In attempting to develop a system by which an accurate IED picture can initially be developed and subsequently sustained, one approach could be to work off a definition of an IED. While several definitions of an IED are in use, with varying degrees of accuracy and often scripted for specific audiences or contexts, one that is a good fit to generically describe this weapons system is given by: a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores but is normally devised from non-military components.[1] However, there are aspects of IEDs, and their use not captured in this definition, that would be needed to base an IED threat picture around. For example, IEDs possess the characteristic of being clandestine which is not captured in this definition. As previously noted, definitions of IEDs are often tailored to specific audiences or contexts, resulting in multiple definitions, with little likelihood of consensus within the international C-IED community. This highlights the inherent difficulty in creating a methodology to construct an IED threat picture based solely on a definition.

A more systematic approach to understand IED use in a given context involves examining IED attacks under the headings of their what, how, where, when, who and why. More precisely a comprehensive understanding of the following is required:

- What components make an IED?
- Where are IED attacks likely to take place?
- When are IED attacks likely to take place?
- Who is involved in IED attacks?
- Why are IEDs being employed?
- How are IEDs being employed?

1 United Nations Office for Disarmament Affairs (UNODA) International Ammunition Technical Guidelines (IATG) dated April 2011.

This understanding can be considered the 5W+H of IEDs. This comprehensive analysis helps to attain an understanding of the threat, develop IED analysis tools, and maintain an accurate IED threat picture. Such an approach, helps identify the strengths and weaknesses of an IED system, enabling a threat-aligned C-IED enterprise to make well-informed decisions regarding investments in effective counter-IED efforts. Several subsequent articles in The Counter-IED Report will examine the 5W+H of IEDs as a process in creating a flexible yet systematic approach to developing and maintaining an IED threat picture. This article, however, focuses on examining some common methods used to classify IEDs. It will outline how IEDs and their employment can be analysed from multiple perspectives, each emphasizing particular aspects of their design and use. A key message is that while each classification method has its merits, engaging more than one method of classification allows for a more comprehensive understanding of the technical complexity of IEDs in use. We will begin by discussing the importance of exploring different methods for classifying IEDs, which are essential to developing and maintaining an accurate IED threat picture. A supporting information management system will play a key role in this process, inevitably requiring a database to efficiently organize and manage the necessary data.

DATABASES IN SUPPORT OF AN IED THREAT PICTURE

Any IED threat picture will need to be based upon accurate information of sufficient detail on IED use, the IED system employing them and the context of their use. This will require the capture of data related to these three elements of the IED threat picture and its subsequent analysis as part of some process or intelligence cycle. This will ultimately produce IED intelligence products which can then be used to support the understanding of the C-IED enterprise so that the C-IED efforts invested in remain threat aligned at all times. In terms of IED use, there is a need to understand their technical complexity and their tactical employment. This will necessitate the capture of IED incident data and its input into a database. Databases of IED information and intelligence can be used to find and compare IED incidents. Over time, as the dataset is grown, this will allow for trends, patterns and insights to be obtained. It is such trends, patterns and insights that are needed to develop and sustain an accurate IED threat picture. For an IED database to be useful in informing an IED threat picture, all data entered needs to be structured, systematic and consistent. While advanced comprehensive databases can be designed, some of the challenges which need to be considered include:

- The vast number of IEDs in terms of their technical complexity and how they can be used in terms of their tactical employment is immense and is a challenge to cover every possible scenario.
- The acceptance of the likely threat evolution over time owing to action-reaction-counteraction cycle between the IED system and those engaged in the C-IED enterprise.
- The need for non-specialists in database management, data entry and IEDs to be able to engage with the database in a user friendly and intuitive manner requiring minimal training to do so.

It is for these reasons that when designing an IED database that a systematic and as comprehensive as possible, without being overly complex, system is needed. Applying the KISS principle[2] in IED database design is a good approach. This is where the use of IED classification systems can be useful to assist with this challenging endeavour.

2 Keep It Simple and Structured as possible.

IED CLASSIFICATION METHODS

IEDs can be classified[3] in multiple ways to account for a large number of design possibilities and tactical employment methods.[4] It is unrealistic for every possible IED to be described. However, by applying the KISS principle and utilizing generic classifications with specific examples, it becomes possible to systematically classify IEDs in various ways that are both flexible and practical. The IED threat picture developed and sustained by a C-IED enterprise will ideally speak to its stakeholders which will include specialists and non-specialists at the strategic, operational, and technical / tactical levels. These various audiences will have varying requirements which should ideally be accounted for. By considering IEDs under the following four classifications, a large number of variations is reduced to a manageable number of generic classes which provides understanding for the various stakeholders within the C-IED enterprise and their different requirements:

- Method of actuation
- Tactical employment
- Target effect
- Technical components

An examination of the first three means of IED classification is provided below with the fourth, classification by technical components, the subject of a subsequent article examining what components make up an IED. We will conclude by examining the issue of classification crossover, emphasizing that the various means of classifying IEDs should not be viewed as isolated or mutually exclusive. Instead, the importance of adopting a flexible and context-driven approach when classifying IEDs is advocated, ensuring that the classification applied best highlights the relevant characteristics within a given context.

Method of Actuation Classification

IEDs can be classified by their actuation method[5] which refers to how the IED is designed to be initiated. IEDs can be classified by one of three methods of actuation, namely, time, victim-operated, and command. Below an argument is set out that suicide IEDs are a special category of command IEDs; however, in some systems they are considered as a fourth method. Understanding the method of actuation can provide insight into the most appropriate defeat the device capabilities to be invested in. These three categories of IED actuation method, are also the three categories of IED switch, which can be either a firing or arming switches. IED switches are one of the elements captured under the technical components of an IED.

3 The act of arranging or organizing a set of objects into groups based on common attributes, characteristics, qualities, traits, capabilities, or features.

4 A description of how the device and target were brought in proximity of each other. The IED Incident Reporting Guide, 6th Edition.

5 The terms operation and actuation are sometimes used interchangeably when referring to how an IED is initiated; however, actuation and operation have distinct meanings, particularly in technical contexts. Actuation refers to the process of turning on, starting, activating[i] or triggering[ii] any mechanical, electrical, electronic or chemical device or system. Mechanical actuation can involve turning on or off a motor, opening or closing a valve, moving a lever or switch, and initiating a mechanical timer. Electrical actuation can involve switching on or off an electrical circuit, activating a relay or contactor, powering an electrical device, triggering an electrical signal or alarm, and initiating an electrical process, such as a heating element. Electronic actuation can involve activating a semiconductor device such as a transistor, powering on an electronic circuit, triggering a digital signal or process, engaging an electronic control system and starting an embedded system or microcontroller. Chemical actuation can involve initiating a chemical reaction, starting a catalytic process, activating a chemical sensor or detector and triggering a chemical release mechanism. Actuation focuses on the initiation step. On the other hand, operation refers to the overall functioning or performance of a device or system. It encompasses the entire process from start to finish, including actuation, control, and execution of the intended task. For example, the operation of a machine includes not only turning it on (actuation) but also all the steps involved in its functioning until it completes its task.

   i. Activation can imply turning on a system or process, making it ready for operation and is frequently used in the context of electrical and chemical devices or systems.

   ii. Triggering is used to refer to causing an event or action to occur, often used in electronics to start a sequence or response.

Time

Time IEDs are those which function after a pre-determined period of time has elapsed. An IED fired after the passing of time allows attackers to be at a safe distance at the moment of initiation, and to escape the scene before security forces can respond. Time IEDs are suitable for static targets such as buildings and installations but limited against moving targets. Another disadvantage of time IEDs is that the intended victims might not be within the danger area when it initiates. However, they still pose a serious threat as tactics can be employed which, draw an unwary target into loitering near it when initiated or they can be employed in indiscriminate attacks, targeting anybody present at a certain location and time.

Victim Operated

A victim-operated IED is an IED with a firing switch that is activated by the actions of an unsuspecting individual, relying on the victim to carry out some form of action that will cause it to function. This method offers the attacker a means to ensure the target is close to the IED when it initiates. The main challenge for the attackers is to find circumstances in which only an intended target will trigger the IED, i.e., an innocent person will not inadvertently trigger it. However, victim operated IEDs may be employed in indiscriminate attacks, targeting anybody at a certain location and time. Victim-operated switches may also be incorporated into IEDs as a secondary means of actuation to target those who attempt to defeat the device.

Command

Command IEDs are those which allow an attacker, often called the triggerman or bomber, to initiate it at a moment of their choosing by completing an action that actuates the firing switch. Command IEDs are especially suited to attacking mobile targets. This author contends that, command IEDs can be categorised under:

- Emplaced and remotely initiated IEDs
- Suicide IEDs
  - Bomber initiated
  - Triggerman initiated

The author sees logic considering suicide IEDs, whether involving suicide bombers or proxy bombers, as a form of command IED. This is because their initiation is ultimately controlled by a deliberate action, either by the bomber themselves or by a triggerman monitoring and activating the device remotely. In both cases, a deliberate intended action is necessary to initiate the device. However, delivery of suicide IEDs by a human element adds a layer of complexity that distinguishes them from other command IEDs with their means of employment often needing to be captured also. This highlights the issue of classification crossover which is discussed later.

Emplaced and remotely initiated IEDs

An emplaced[6] and remotely initiated command IED involves an attacker selecting two suitable locations: the contact point where the IED will be emplaced, and the firing point from where the triggerman will initiate the device. An emplaced command IED gives the attacker the means to attack a specific target from a safe distance at a moment when initiation will have optimal target effects. There are many methods to initiate an emplaced command IED. Two common methods are by radio control and by command wire. Other methods are possible, for example, pulling a long string. More obscure command firing switches have been used involving the use of various technologies that allow a triggerman to complete an action that causes a firing switch to function from a distance.

Suicide IEDs

A suicide IED is initiated at an attacker's chosen moment, with an individual carrying the device intentionally killed either as part of the attack or to

6 An IED that is statically placed where it is likely to be encountered by the intended target. The IED Incident Reporting Guide, 6th Edition.

avoid capture. Both suicide bomber and proxy bomber[7] attacks are considered suicide IEDs. The bomber in both cases, is the person involved in transporting or delivering the IED to the point where it is initiated. Suicide IEDs fall under the command actuation method as their initiation ultimately depends on a deliberate action — either by the bomber themselves or by a triggerman remotely controlling the device. This method of command actuation is often closely tied to its delivery mechanism, which may include a person-borne IED (PBIED) or a suicide vehicle-borne IED (SVBIED). Distinguishing between suicide and proxy attacks is frequently challenging until after an attack, leading to significant overlap in the defeat-the-device capabilities developed to counter suicide IEDs.

Bomber Initiated Suicide IEDs

Suicide bomber attacks involve a compliant and cooperative bomber who actively participates in the attack. Suicide bombers provide the ability to circumvent defences by avoiding them and guide an IED to a desired contact point earning them the nickname of 'guided IEDs.' Unless neutralised or they have last minute reservations on completing an attack, a suicide bombers is the triggerman in such attacks. Although, proxy bomber attacks involve someone who is not a willing participant in the attack, they may have been intimidated, threatened, or manipulated through forced substance consumption to activate the device against a given target.

Triggerman Initiated Suicide IEDs

There are various reasons and scenarios why a remote trigger is included either as the primary or secondary means of firing a suicide IED. This allows an attacker, other than the bomber, to act as a triggerman with the ability to initiate the device as the primary or secondary (backup)[8] means of firing. These scenarios include:

- A suicide bomber is neutralised prior to having the opportunity to initiate the device.
- A suicide bomber becomes reluctant to complete their attack.
- A proxy bomber, despite being threatened, intimidated, or drugged does not carry out the directions given to them.
- A proxy bomber is unwittingly delivering an IED to a target.

Tactical Employment Classification

Tactical employment is a means of IED classification, in which IEDs are categorised by how the device and target were brought in proximity of each other. It often refers to the method of delivery allowing an understanding of how an attack was intended to be conducted. Tactical employment of IEDs include vehicle-borne; animal-borne; person-borne (proxy or suicide bomber); emplaced; standoff; water-borne; air-borne; and postal IED. It is noted that both water-borne and air-borne refer to their domain of use as much as any other characteristic and are often considered types of standoff IEDs.

Standoff IEDs are a special category of tactical employment of IEDs for several reasons. For this reason, this category of IEDs will be elaborated on in more detail. Standoff IEDs refer to a method of IED employment, involving an explosive device launched or released by an attacker from a safe location, which then travels to its point of contact. Standoff IEDs enable attackers to engage a target without requiring their presence at the point of contact at any stage of the attack. They also allow for the bypassing of physical security measures, such as barriers that prevent the emplacement or

7 When a suicide IED is delivered by an individual who has been coerced into carrying out the attack or is unknowingly transporting the device to its target, it is classified as involving a proxy bomber rather than a suicide bomber. The level of control and assurance of success with proxy bombers compared to suicide bombers is lower, as the person delivering the device may not act as directed, or if carrying the device unwittingly, may act in an unplanned manner.

8 A 'chicken switch' refers to the use of a secondary firing switch by a triggerman. This serves as a backup to remotely initiate a suicide IED if the bomber hesitates, fails to act, or is neutralized, ensuring the device functions as intended.

delivery of IEDs by other means. Standoff IEDs can be employed across land, air, and maritime domains.

Standoff IEDs can be further classified as unguided and guided. Unguided standoff IEDs, once launched or released, have no means of subsequent control by the attacker. Their targeting relies on their initial positioning, trajectory and often environmental factors that will influence their external ballistics. Unguided standoff IEDs are only suitable for attacking static targets, requiring the attacker to carefully select two locations: its launch or release point and the contact point where it will initiate. They are typically not suitable for attacking mobile targets.

On the other hand, guided standoff IEDs can be controlled in some aspect after launch or release by an attacker, allowing them to adjust their trajectory or placement to a contact point. Examples include remote controlled uncrewed vehicles in the land domain, aerial platforms, more commonly referred to as uncrewed aerial systems (UAS), controlled by an attacker to deliver an IED, and guided surface and subsurface water borne IEDs. Guided standoff IEDs can be used to target both static targets as well as mobile targets. The guidance and control of such standoff IEDs can be linked or unlinked. A linked standoff IED retains a physical link between the attacker at the point of release and the IED,[9] while an unlinked standoff IED is controlled by a remote means, typically involving the use of some band of the electromagnetic spectrum at certain frequencies.

In the land domain, standoff IEDs can be delivered using uncrewed vehicles. These vehicles are typically controlled by the attacker, either through linked or unlinked systems, enabling precise guidance to the desired contact point. However, cases of unguided uncrewed vehicles which were not controlled in terms of their movement once released from their launch / release point have been documented. In such cases it is typical for unguided land based standoff IEDs to remain linked to the attacker to allow for the moment of initiation to be controlled.

In the maritime domain, surface and subsurface standoff IEDs can be guided or unguided once released from their launch point. An improvised torpedo is an example of a subsurface unguided standoff IED. Various improvised surface vessels adapted as IEDs are typically controlled to guide them onto their intended target.

In the air domain, there is a far greater variation of standoff IED types. In terms of unguided air standoff IEDs, they may be further classified as direct or indirect. Improvised projectiles fired directly at a target are examples of direct unguided aerial standoff IEDs. Examples include the Provisional IRA's Mk 16 mortar[10] as well their Projected Recoilless Improvised Grenade (PRIG) and their Improvised Projected Grenade (IPG). Improvised mortars and rockets fired with a lobbed trajectory at a target are examples of indirect unguided aerial standoff IEDs. Balloon-borne IEDs are another example of indirect unguided aerial standoff which upon release rely on wind currents to reach their targets, making them unpredictable but can be effective in certain scenarios. Their use has been documented being released in Gaza to target locations in Israel.[11]

Guided aerial standoff IEDs typically involve some aerial platform (uncrewed aerial system (UAS)[12]) being used to deliver an IED to a target. UAS may be used in a variety of ways in standoff attacks to deliver explosive effects to a target. These systems

9 Examples include firing cable or fibre optic cable remaining attached to an IED or it's delivery platform and unwinding as it moves from the launch / release point to its contact point, retaining a physical connection to the attacker which they use to guide the IED to its target and or control its initiation.

10 The designation of this projected horizontal shaped charge standoff IED is misleading, as it does not align with the characteristics of a mortar, which is defined by its lobbed trajectory from the launch point to the point of contact.

11 https://www.terrorism-info.org.il/app/uploads/2020/01/015_20_E.pdf

12 Often referred to colloquially by the term 'drone' which has become a widely recognized and informal term in common use; however, it is not a precise technical term. Drone is also often used colloquially in the water domain also. UAS in this context is taken to include unmanned aerial vehicles (UAV) and remotely piloted aircraft systems (RPAS).

are controlled by the attacker until a certain point, where they either release their explosive ordnance onto a target, fire at a target, or crash into a target. The act of releasing explosive ordnance by dropping it onto a target is known as improvised aerial bombing. When a UAS is crashed into its target as a one-way attack it is often referred to as a 'kamikaze-drone,' with its explosive payload initiating upon impact.

Target Effect Classification

IEDs can be classified by their intended principal target effect. This classification provides a quick understanding of an attacker's intended purpose of an attack or, alternatively, the 'intended, immediate, or direct tactical effect of an IED'[13] attack. It can be useful in sending a quick report or organising the immediate response to an attack. Possible intended purposes include anti-armour; anti-personnel; anti-air; anti-infrastructure; anti-vehicle; anti-maritime; tactics, techniques & procedures (TTP) identification; obstacle creation; breaching.

CLASSIFICATION CROSSOVER – FLEXIBLE AND CONTEXT-DRIVEN APPROACH

When classifying IEDs, it is essential to recognize that the various means of classification are not isolated or mutually exclusive. Certain IEDs can fall under multiple categories, depending on the perspective or the lens through which they are being examined. This overlap highlights the importance of avoiding a siloed approach to classification. Instead, the chosen classification should reflect the characteristics most relevant to the context or the specific aspects that need to be emphasized. It is also often advantageous to consider IEDs under multiple systems of classification, especially when addressing more complex devices. These IEDs may exhibit characteristics that overlap across different classification systems, such as their method of actuation, tactical employment, and target effect.

The fact that suicide IEDs are often closely tied to their delivery mechanism, which may include a person-borne IED (PBIED) or a suicide vehicle-borne IED (SVBIED) is an example of the merit of using more than one classification systems for certain IEDs. Examining standoff IEDs further illustrates the reality of IED classification crossover. Classification of standoff IEDs can be complicated owing to the large number of switch types that can be used to launch the IED, arm it and then cause it to initiate i.e. the firing switch. For example, command launch, delay armed, timed aerial burst standoff IEDs have been documented. Firing switch classification can become even more challenging when conventional items of explosive ordnance are employed and function in their original design role e.g. impact initiated or time delay after release. For example, light dependant resistors have been employed to allow for the time delay launch of unguided conventional rockets from improvised launch platforms which function by activation of their conventional impact fuze. A UAS employed standoff IED, may have a timed (delay) arming switch activated after release, with a conventional fuze functioning upon impact into its target. Integration of improvised firing switches with conventional items of explosive ordnance is also known. Hybrid switches[14] are often used with aerial standoff IEDs. For example, secondary timed switches can be integrated into standoff IEDs to prevent their capture and subsequent technical exploitation. This can be taken even further with secondary victim operated switches integrated to target any person trying to recover the IED and prevent its exploitation. Classifying an IED as standoff offers valuable insight into its tactical employment. However, this classification can be further refined by incorporating

13 The IED Incident Reporting Guide, 6th Edition.

14 A hybrid IED switch refers to any switch or number of switches configured as a combination of timed and/or command and/or victim operated switches to act independently and/or dependently on each other.

details such as the domain of operation, launch method, arming method, and, where applicable, the specifics of primary and secondary firing switches. This expanded approach adds greater depth and precision to the classification.

By utilizing more than one means of classification when examining IEDs, analysts can more comprehensively capture the features of devices. Detailed understanding of the interplay between delivery and actuation of an IED is particularly valuable in C-IED efforts, as it empowers informed decision making for effective defeat the device capabilities. By adopting a flexible and context-driven approach, IED classification can remain both practical and insightful. Describing an IED through more than one method of classification allows for a more comprehensive understanding of their technical complexity which is a key part of any IED threat picture and in turn informs an understanding of the threat.

CONCLUSION

As part of series of articles examining a methodology for the development and sustainment of an IED threat picture, this article has outlined three IED classification systems in use. It has also introduced the need for a comprehensive understanding of the 5W+H of IEDs to develop such a methodology. Several subsequent articles in *The Counter-IED Report* will examine the 5W+H of IEDs as a process in creating a flexible yet systematic approach to developing and maintaining an IED threat picture. These six considerations of IEDs will work from the technical (what) to the tactical (how) levels before moving to more operational aspects (where and when and who) prior to examining strategic level considerations (why). The examination of what components make up and IED is linked to the subject of this article, using the fourth named IED classification – technical components. This is the topic of the next article in this series in the curiously titled a 'Journey Through PIECES of SPICE PIES.' ■

ABOUT THE AUTHOR

Paul Amoroso is an explosive hazards specialist and has extensive experience as an IED Threat Mitigation Policy Advisor working in East and West Africa. He served in the Irish Army as an IED Disposal and CBRNe officer, up to MNT level, and has extensive tactical, operational, and strategic experience in Peacekeeping Operations in Africa and the Middle East. He has experience in the development of doctrine and policy and was one of the key contributors to the United Nations Improvised Explosive Device Disposal Standards and the United Nations Explosive Ordnance Disposal Military Unit Manual. He works at present in the MENA region on SALW control as well as in wider Africa advising on national and regional C-IED strategies. He has a MSc in Explosive Ordnance Engineering and an MA in Strategic Studies. He runs a consultancy, Assessed Mitigation Options (AMO), which provides advice, support, and training delivery in EOD, C-IED, WAM as well as Personal Security Awareness Training (PSAT) and Hostile Environment Awareness Training (HEAT). This article reflects his own views and not necessarily those of any organisation he has worked for or with in developing these ideas.

LinkedIn profile: https://www.linkedin.com/in/paul-amoroso-msc-ma-miexpe-60a63a42/

A JOURNEY THROUGH PIECES OF SPICE PIES

WHAT COMPONENTS MAKE UP AN IED - TECHNICAL COMPONENT CLASSIFICATION

By Paul Amoroso, an explosive hazards specialist at Assessed Mitigation Options (AMO) consultancy

INTRODUCTION

This is the third article in a series examining how to develop and sustain an accurate IED threat picture to optimize understanding and ensure the C-IED efforts invested in remain effective as threats evolve. The first article titled, 'Understanding and Threat Alignment Within a C-IED Enterprise' emphasised understanding as a vital cross-cutting element of any C-IED enterprise, encompassing two key aspects: the threat itself and the effectiveness of the C-IED efforts invested in. The rest of this series of articles will focus on understanding the threat of IED attacks, through an IED threat picture.

To systematically understand the use of IEDs by a specific network in a given context[1], it is essential to analyse IED attacks using the following key questions: what, how, where, when, who, and why. More precisely a comprehensive understanding of the following is required:

- What components make up an IED?
- Where are IED attacks likely to take place?
- When are IED attacks likely to place?
- Who is involved in IED attacks?
- Why are IEDs being employed?
- How are IEDs being employed?

This understanding can be considered the 5W+H of IEDs. This comprehensive analysis helps to attain an understanding of the threat, develop IED analysis tools, and maintain an accurate IED threat picture. By doing so, the strengths and weaknesses of the IED network can be identified, contributing to a threat aligned C-IED enterprise empowered to make informed decisions on investment in effective C-IED efforts.

Along with several future articles in The Counter-IED Report, this article will explore the 5W+H of IEDs as a process to create a flexible yet systematic approach for developing and maintaining an IED threat picture. It examines one of the previously mentioned methods of IED classification[2] – technical components as a means to explore the first question of the 5W+H, 'what components make up an IED.'

Understanding the IED components in use is vital to informing multiple C-IED efforts involved in any C-IED enterprise. Most notably, this will inform the most appropriate IED defeat the device capabilities that need to be invested in, developed and sustained. It will also be the most vital information around which all efforts to control IED components will be based. We

1 Context in terms of an IED threat picture refers to both the IED system involved and the local context. The IED system is assessed under its intent, capabilities and the opportunities it has to employ IEDs against defined target(s). Local context is defined by a geographic area, the target of the attacks and other local factors.

2 IED Classification – Breaking Down Bomb Attacks, The Counter-IED Report, Spring/Summer 2025.

will explore how this question can be addressed by recognizing that different levels of detail may be applied when answering it. A progressively detailed examination of IED components will be structured using three simple mnemonics, each providing a simple memory aid to assist in systematic profiling of IED components. Each mnemonic provides an increasingly comprehensive framework for IED technical component categorisation, the simplest being PIES, followed by SPICE, with PIECES being the most comprehensive. This examination involves a journey through PIECES of SPICE PIES. We will first examine a question often asked by many when initially being briefed on the threat posed by IEDs, 'what does an IED look like?'

WHAT COMPONENTS MAKE UP AN IED?

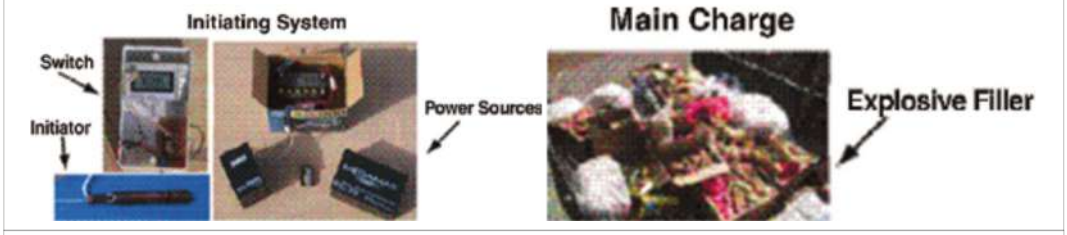
A recurrent question often asked when briefing or delivering training to those involved in various C-IED efforts, is 'what do IEDs look like?' In many cases the audience are not C-IED specialists but from law enforcement, first responders, all-arms military units, borders and customs control, local international NGOs, government officials, members of the judiciary and even IED affected communities.

Examining how to address this question without creating false awareness through overly specific or prescriptive descriptions is a crucial starting point. The answer provided by this author to date has been that an IED most likely resembles its container,[3] which, due to its improvised nature, can take on an almost limitless variety of items. This highlights the significant challenge in systematically classifying the technical components of IEDs, a challenge rooted in their inherently improvised nature, in that an IED can in theory be constructed from a vast array of components.

PIES

The basic components needed for any IED involve some explosive train, a switch to cause it to function and typically a power source.[4]

The explosive train will typically involve both a main charge and an initiator. This provides the basis components of most IEDs, to typically include explosives, an initiator, one or more switches, and a power source. These four components can be arranged to make the mnemonic PIES, referring to Power source; Initiator; Energetic materials;[5] and Switches – both firing and arming if present.



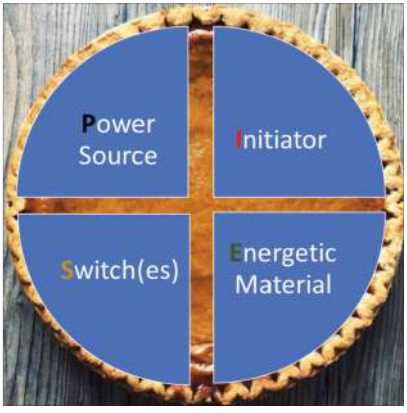
An online graphic[6] outlining the components of an IED – in this case the term initiating system is used to describe the switch, initiator and power source.

3 In most cases, the container of an IED can be any item with a void within which the other components are secreted or held. A container may also act to have some of the IED components attached to it.

4 The author acknowledges that it is possible to have an IED without a power source in the traditional sense with such IEDs having been documented; however, they are rare and difficult to employ effectively, typically owing to the sensitivity of the energetic material involved.

5 The term "explosives" is often used in this context to refer specifically to the main charge. However, in a broader sense, it encompasses all energetic materials in the IED, apart from the initiator. Within the PIES framework, the "E" accounts for these energetic materials, which can include high explosives, propellants, and pyrotechnic compositions. Consequently, the "E" in all three mnemonics refers to any energetic material involved.

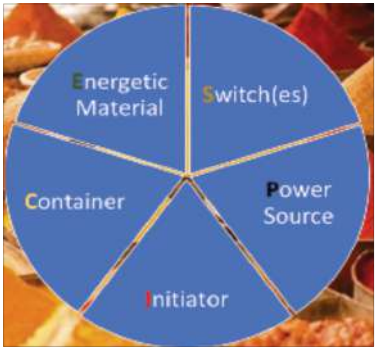
6 Images from Examining the Role of Metadata in Testing IED detection System, by Paul J. Fortier and Kiran Dasari University of Massachusetts Dartmouth, Published in the ITEA Journal 2009: 30: 421-433



Under each of the technical headings of power sources, initiators, energetic material and switches various further classification is possible, leading to a hierarchy of technology[7] As a basic example, the type of firing switch, can be further classified as command, time, victim operated or hybrid.[8] This concept of a hierarchy of technology can be applied to categorizing the components of IEDs by organizing them into levels based on their functionality, complexity, and importance within the device. This approach helps in systematically analysing and understanding the construction of IEDs, providing clarity to their diverse and improvised nature. A systematic and detailed classification system of how power sources, initiators, energetic material and switches can be further categorised, along with extensive examples, is provided in '*The IED Incident Reporting Guide*,' 6th Edition,[9] and also reproduced in Annex A-Lexicon of the UN IED Threat Mitigation Handbook, Second Edition, 2024.

SPICE

When we consider the components accounted for under the PIES headings, we may return to the question posed earlier – what does an IED look like? The answer to which, is that it typically looks like its container. So, we may need to account for an IED's container when considering its components. When we do this, we can use the mnemonic SPICE, standing for Switch(es), Power-source, Initiator, Container and Energetic material.



From a technical perspective, in addition to a general description of an IED,[10] the key characteristics of a container that need to be captured are any aspects which contribute to the IED's concealment or explosive effects. Concealment characteristics of an IED container refer to 'materials used to prevent the discovery of an IED by visual inspection.'[11] Explosive effects characteristics of a container refer to aspects such as:

- Confinement of an explosive main charge which may lead to a deflagration to detonation effect and is often how pipe bombs function.
- Configuration of the container to produce directed explosive effects which are considered a type of enhancement and are covered later in this article.

7 The term "hierarchy of technology" refers to the structured arrangement or classification of different technological systems, tools, or components based on their complexity, functionality, or importance. This hierarchy often highlights the relationship between foundational technologies that serve as building blocks and more advanced technologies that depend on or are built upon them.

8 A hybrid IED switch refers to any switch or number of switches configured as a combination of timed and/or command and/or victim operated switches to act independently and/or dependently on each other.

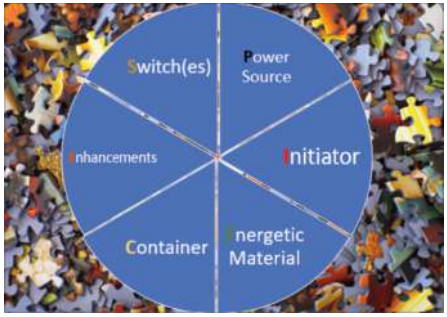
9 https://tripwire.dhs.gov/carousel/ied-reporting-guide-6th-edition Released January 2024.

10 For example, the use of certain containers in some areas has given rise to generic descriptions based upon the container in use such as coffee jar IED.

11 The IED Incident Reporting Guide, 6th Edition.

PIECES

While the SPICE mnemonic accounts for the main components in an IED it fails to account for components which are often of greatest interest – enhancements.[12] The inclusion of enhancements leads to the mnemonic PIECES, standing for Power-source; Initiator; Energetic material; Container; Enhancements; and Switch(es).



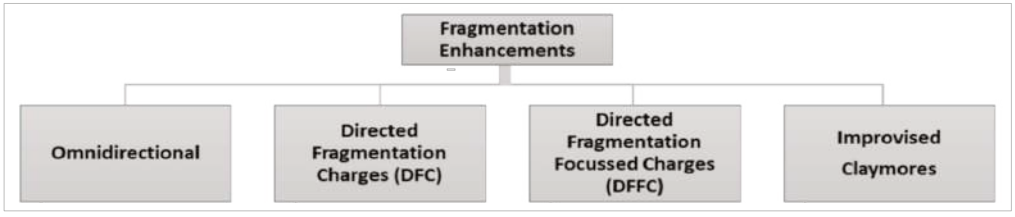
It is acknowledged that not all IEDs have enhancements, with some IEDs producing all their explosive or incendiary effects from the main charge. An IED can be considered enhanced when additional material is integrated into the main charge, positioned in close proximity to it, or when the main charge is configured in a specific way relative to the container or added items. Enhancements are added to an IED to increase their harmful and damaging effects. The following six types of enhancements are possible:

- ***Blast enhancements***

  The blast from some common explosives can be increased by mixing certain material with them. Common terms associated with such IEDs are blast bombs and enhanced blast IEDs.

- ***Fragmentation enhancements***

  The effects of blast reduce quickly with distance from the point of initiation, with the container of an IED often producing natural fragmentation which along with other components are propelled omnidirectionally from the point of initiation often causing many of the injuries and in certain cases damage. For example, a pipe bomb propels often lethal fragmentation in the surrounding area due to the rupture and projection of the container material. The effects of fragmentation can be increased by the addition of additional often metallic material to an IED. This gives rise to such descriptors as nail bombs, ball bearing IEDs etc. Such omnidirectional fragmentation charges can cause casualties in all directions. Alternatively, fragmentation may be positioned to channel fragments into a narrower path, functioning similarly to a large shotgun, forming what is known as a Directional Fragmentation Charge (DFC) and sometimes referred to as shotgun IEDs. A variation on this design is to produce a curtain of fragmentation projected out from one side of an IED. Such IEDs are often referred to as claymore IEDs or improvised claymores. Another variation on the DFC design is a Directed Fragmentation Focussed Charge (DFFC) designed to project fragments to a point of optimal concentration some distance from the IED. This allows us to classify IED fragmentation enhancement under four sub headings as shown below.

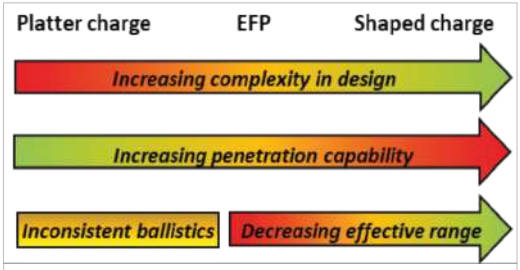


12 An optional, deliberately added component or configuration of the IED as opposed to a secondary hazard which modifies the effects of the IED. The IED would be effective yet produce a different measurable result if this material or configuration was not present. The effect can be additional physical destruction, proliferation of dangerous substances (radiation, chemicals, etc.), or other results to enhance the effect of the IED. The IED Incident Reporting Guide, 6th Edition.

- ***Directional explosive effect enhancements***

IEDs can be enhanced for the purpose of attacking armoured vehicles, including blast-resistant armoured vehicles, by the use of directional explosive effect[13] enhancements. Such IEDs concentrate explosive force onto a plate, metal disk or liner which is projected at the target. They can have various degrees of technical construction from loosely fitted flat plates to well-engineered copper cones with resulting variations in complexity of design, effective range, and penetrative capability. There are three basic types of directional explosive effect enhancements:

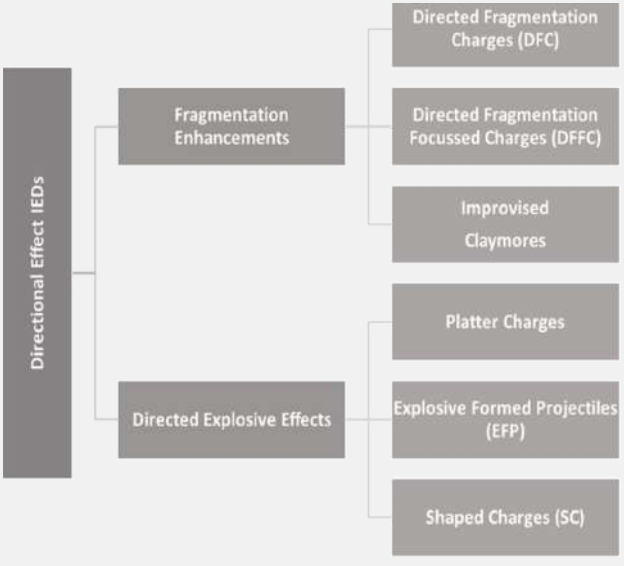
- Platter charges;[14]
- Explosively formed penetrators (EFPs);[15]
- Shaped charges (SC).[16]



Variation in characteristics of directional explosive effect enhancements.

Directional Effect Enhancements

Platter charges, EFP and SC are all examples of directional effect IEDs. The term directional effect IEDs is one that refers to IEDs which have either directional explosive effects, such as platter charges, EFP and SC as well as those with directed fragmentation effects such as DFC, DFFC and improvised claymores. This is an example of the overlap that can occur when classifying enhancements. The classification system employed may choose separate categories of fragmentation enhancements and directed explosive effects of have them combined under the broader directional effect category.



13 A term used to describe explosive effects produced by the initiation of explosives in intimate contact with a liner which is projected forward with varying effects depending on many factors resulting in either shaped charge jets, Explosively Formed Projectiles (EFP) or platter charges.

14 In a platter charge IED, the enhancement is added in the form of a flat metal plate. When the IED is initiated, the plate is projected towards the target at high velocity, often breaking into several large fragments. The plate, or fragments, may be capable of penetrating light armour at distance of a few metres.

15 Also referred to as explosively formed projectiles, explosively forged projectiles and explosively forged penetrators. In an EFP IED, the enhancement is added in the form of a dish, precisely shaped from ductile metal. When the IED is initiated, explosive forces bend the dish causing it to invert. This forms a smaller more aerodynamically stable cross-sectional area penetrator that is projected towards the target at very high velocity. Depending on their design, these projectiles are capable of penetrating substantial armour at distances even beyond 10 m or so.

16 Shaped charges are common in conventional munitions, often referred to as HEAT warheads. In a shaped charge IED, the enhancement often involves the addition of a copper cone. When the IED is initiated, a jet of copper is fired towards the target at extremely high velocity. Jets can penetrate very thick armour, but only if the IED is initiated in close proximity to its target.

- ***Incendiary enhancements***

  IEDs can be enhanced by the addition of flammable liquids for the purpose of increasing casualties or starting fires in buildings. Unconfined, much of the effect of fuel enhancement will result in a fireball which will lead to thermal injuries to those within the danger area. When initiated inside a building or in close proximity to flammable material, the effects are often much more destructive than the use of explosives alone. The term blast incendiary is sometimes used to describe such devices.

- ***Chemical Biological & Radiological (CBR) enhancements***

  IEDs can be made more terrifying by adding Chemical, Biological, or Radiological (CBR) enhancements. The explosive blast of CBR-enhanced IEDs, is designed to disperse chemical, biological, or radiological substances into the surrounding area. This results in contamination of the area with toxic materials, exposing those present at the time of initiation as well as potentially those responding to such an attack. Broadly there are three categories of CBR enhancements. Those which are improvised, those which involve the use of commercial toxic materials[17] and those which are military or weaponised agents.

Chemically enhanced IEDs may involve the use of improvised chemicals,[18] toxic industrial chemicals[19] or military grade weaponised chemicals also referred to as chemical warfare agents (CWA).[20] For example, an explosive charge may be attached to cylinders of chlorine, with the intent that upon initiation, chlorine is released into the atmosphere. Attempts to use the CWA mustard gas (sulphur mustard)[21] have been documented as well as efforts to employ the nerve agent sarin;[22] however, the development of such complex and relatively unstable CWA is not easily achieved, typically requiring specialist equipment and high-level competent chemists and engineers. This makes improvised CWA production limited in terms of quality and quantity and often restricted to certain industrial facilities and in some cases research institutes.

Radiologically enhanced IEDs may involve the use of toxic industrial radiological materials.[23] The use of an IED to explosively disseminate radiological particles is often referred to as a ‘dirty bomb’.

17 Generic term for toxic or radioactive substances in solid, liquid, aerosolized, or gaseous form that may be used, or stored for use, for industrial, commercial, medical, military, or domestic purposes. Toxic industrial material may be chemical, biological, or radioactive and described as toxic industrial chemical, toxic industrial biological, or toxic industrial radiological. Source: The IED Incident Reporting Guide, 6th Edition.

18 This category stands apart from the use of commercial toxic industrial materials and military-grade weaponized CWA sources due to its improvised nature and reliance on non-standard or improvised components. One may consider these as analogous to improvised explosives in comparison to commercial explosives and military grade explosives.

19 A chemical developed or manufactured for use in industrial operations or research by industry, government, or academia. For example: pesticides, petrochemicals, fertilizers, corrosives, poisons, etc. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for human use. Hydrogen cyanide, cyanogen chloride, phosgene, and chloropicrin are industrial chemicals that can also be military chemical agents. Source: The IED Incident Reporting Guide, 6th Edition.

20 A chemical substance which is intended to kill, seriously injure, or incapacitate mainly through its physiological effects. The term excludes riot control agents when used for law enforcement purposes, herbicides, smoke, and flames. Source: The IED Incident Reporting Guide, 6th Edition.

21 https://news.un.org/en/story/2023/06/1137492; and https://ctc.westpoint.edu/islamic-state-chemical-weapons-case-contained-context/

22 https://worldview.stratfor.com/article/sarin-shell-who-might-have-used-it; and https://www.newsweek.com/ieds-secret-sarin-supply-129165

23 Toxic Industrial Radiological (TIR) enhancement refers to any radiological material manufactured, used, transported, or stored by industrial, medical, or commercial processes. For example, spent fuel rods, medical sources, etc. Source: The IED Incident Reporting Guide, 6th Edition.

Biologically enhanced IEDs may involve the use of toxic industrial biological materials[24] or military grade weaponised biological warfare agents (BWA).[25] The explosive dissemination of a biological agent is unlikely to be effective with the same challenges present for BWA production as faced with CWA production. However, this does not mean an attacker with the intent and capability will not attempt to use biologically enhanced IEDs.

The lethality of a dispersed CBR agent in an area depends on its concentration. However, its use often has a profound psychological impact – not only on those within the immediate area but also on people beyond it, especially when news of the attack, particularly if filmed, spreads widely. CBR-enhanced IEDs are primarily designed to terrorise a target group, and it is this impact that makes them a significantly impactful category of IED compared to others.

The acronym PIECES framework is useful for classifying all the possible technical components of IEDs, recognizing that not all IEDs will include all six components. The merits of the PIECES framework lie in its applicability at both the technical level and in supporting efforts to control access to IED components.

The utility of the PIECES nmemonic framework for IED component identification is illustrated above, with the components shown in transit prior to assembly into an IED.

CONCLUSION

As part of series of articles examining a methodology for the development and sustainment of an IED threat picture, we have examined the first question within the 5W+H of IEDs – what components make up an IED? Three simple mnemonic tools of increasing detail have been outlined that can be used when designing an IED database to systematically and consistently capture details of IED components in use in a structured manner. It is advocated that the PIECES framework is employed when profiling IED components, with the caveat that

24 Any biological material manufactured, used, transported, or stored by industrial, medical, or commercial processes which could pose an infectious or toxic threat. Source: *IED Incident Reporting Guide*, 6th Ed, Jan 24.

25 A microorganism or a toxin[A] derived from it that causes disease in personnel, plants, or animals or causes the deterioration of materiel.

NOTE A: A toxic substance produced by and derived from plants and animals or created synthetically. Source: The IED Incident Reporting Guide, 6th Edition.

there is acknowledgment that not all IEDs have all six components present. The merits of the use of the PIECES framework are that it is not only applicable at technical level, but it can also support IED component control efforts. As trends and patterns of the components in use and their technical configuration emerges, device profiling is empowered which can then inform the technical complexity of the threat. Details of the technical complexity of an IED threat is one of the key components that will make up an IED threat picture. The next article in this series will examine the tactical sophistication of IEDs in use by exploring the question, 'how are IEDs being employed?' ■

ABOUT THE AUTHOR

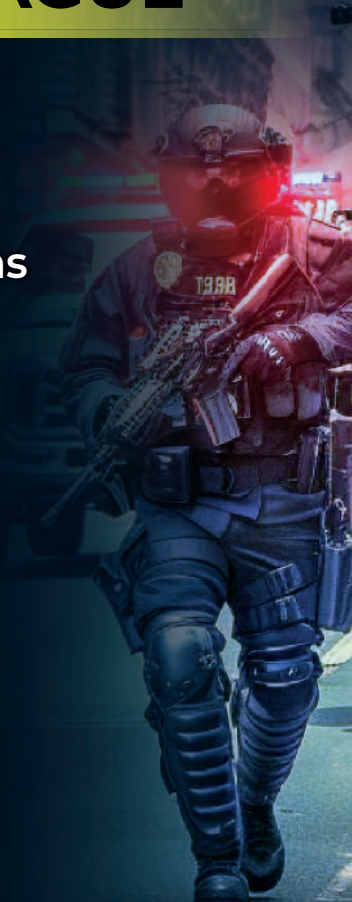
Paul Amoroso is an explosive hazards specialist and has extensive experience as an IED Threat Mitigation Policy Advisor working in East and West Africa. He served in the Irish Army as an IED Disposal and CBRNe officer, up to MNT level, and has extensive tactical, operational, and strategic experience in Peacekeeping Operations in Africa and the Middle East. He has experience in the development of doctrine and policy and was one of the key contributors to the United Nations Improvised Explosive Device Disposal Standards and the United Nations Explosive Ordnance Disposal Military Unit Manual. He works at present in the MENA region on SALW control as well as in wider Africa advising on national and regional C-IED strategies. He has a MSc in Explosive Ordnance Engineering and an MA in Strategic Studies. He runs a consultancy, Assessed Mitigation Options (AMO), which provides advice, support, and training delivery in EOD, C-IED, WAM as well as Personal Security Awareness Training (PSAT) and Hostile Environment Awareness Training (HEAT). This article reflects his own views and not necessarily those of any organisation he has worked for or with in developing these ideas.

LinkedIn profile: https://www.linkedin.com/in/paul-amoroso-msc-ma-miexpe-60a63a42/

Future Forces
EXHIBITION & FORUM

21 – 23 OCT 2026 | PRAGUE

International gathering
of experts, presentations
of technologies and solutions
for security and defence



FUTURE FORCES FORUM

www.FFF.global

General Partner

CSG Czechoslovak Group

EOD / IED & COUNTERMINE SYMPOSIUM

KEY DISCUSSION TOPICS

+ ENABLING WARFIGHTER PROTECTION WITH INNOVATIVE CAPABILITIES
+ MITIGATING THE EVOLVING THREAT: THE PUBLIC SAFETY BOMB TECHNICIAN'S ROLE
+ UNDERSTANDING ENERGETIC AND ORDNANCE COMPONENTS TO SUPPORT EOD AND C-IED EFFORTS
+ COUNTERING THE RANGE OF CBRN AND EOD THREATS IN MULTI-DOMAIN OPERATIONS
+ DEVELOPING AND IMPLEMENTING MITIGATIONS TO COUNTER THE GROWING THREAT OF IEDS AND INCREASE RESILIENCE ACROSS THE HOMELAND
+ EXPLORING THE EVOLVING ROLE OF NAVY EXPEDITIONARY COMBAT FORCES IN COUNTER-IED AND COUNTERMINE MISSIONS

20+ SPEAKERS | **12+** SESSIONS | **5+** SESSIONS

ACTIVE-DUTY US MILITARY/GOVERNMENT ATTEND FREE | COUNTERMINE.DSIGROUP.ORG

JULY 16-17, 2025 | NATIONAL HARBOR, MD

"OLD?" C-IED FOR A "NEW?" ALLIED CONCEPT: THE C-IED APPROACH IN THE LIGHT OF NATO WARFARE DEVELOPMENT IMPERATIVES

By Lieutenant Colonel Jose M Rufas, Chief of Attack the Networks Branch, C-IED Centre of Excellence

"You realize that our mistrust of the future makes it hard to give up the past."
(Chuck Palahniuk in his book "Survivor", first published in 1999)

If you, dear reader, have been reading about the North Atlantic Treaty Organization (NATO), most probably you would be familiar with hearing (and even harder to effectively understand…) terminology such as "*comprehensive approach*", "*countering improvised explosive devices*", "*enhanced forward presence*", "*integrating gender perspective as a force multiplier*", "*attack the networks*", "*innovation continuum*" or "*grey zone*"..

So lately, under the umbrella of "*countering hybrid threats*" approach and in the context of the NATO "*Warfighting Capstone Concept*", the NATO "*Warfare Development Agenda*" (WDA) framework emerges…

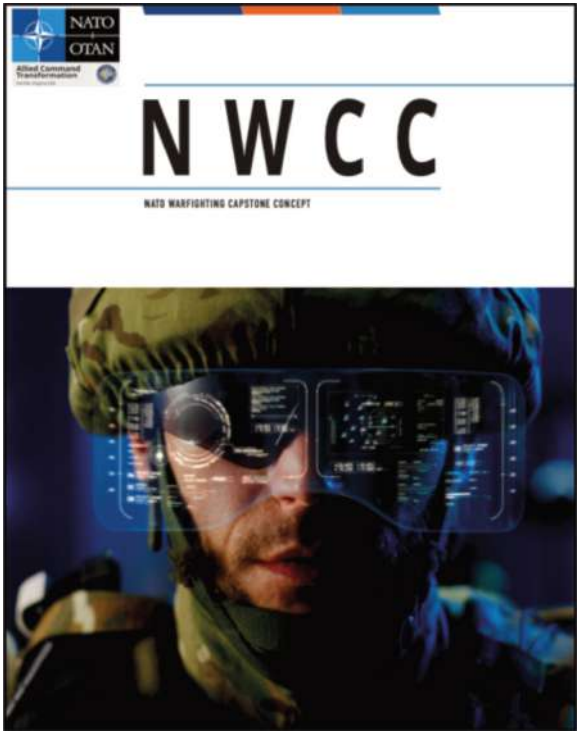


Figure 1: Cover of "NATO Warfighting Capstone Concept" document, as published in 2021 *(Source – www.act.nato.int)*

D'où venons-nous? Que sommes-nous?...[1]

Despite the strong focus of the Alliance on the Russian threat at the Eastern Front, the NATO Strategic Concept 2022 was still considering terrorism as one of the main threats for the Alliance.

34. Countering terrorism is essential to our collective defence. NATO's role in the fight against terrorism contributes to all three core tasks and is integral to the Alliance's 360-degree approach to deterrence and defence. Terrorist organisations threaten the security of our populations, forces and territory. We will continue to counter, deter, defend and respond to threats and challenges posed by terrorist groups, based on a combination of prevention, protection and denial measures. We will enhance cooperation with the international community, including the United Nations and the European Union, to tackle the conditions conducive to the spread of terrorism.

Figure 2: Capture from "NATO Strategic Concept" page 8, as published in 2022 *(Source – www.nato.int)*

Additionally, the last Annual Report from the NATO Secretary General (as published some days before the publication of this article) is making direct reference not only to terrorism but also directly to C-IED and Technical Exploitation…

In other words: do you know about any terrorist group which has been/is not employing or willing to employ improvised explosive devices as a weapon of choice?

Between the lines, we could read and understand how the Countering Improvised Explosive Devices (C-IED) approach could persist as absolutely necessary even without any casualty as directly caused by the detonation of any IED over allied troops. In fact, C-IED is based on the integration, synchronization and coordination of actions seeking for anticipation in benefit of the reduction of capabilities of adversary human networks in the aim of denying them the potential manufacture and use of those devices.

Terrorism: Remaining Vigilant

Terrorism remains the most significant asymmetric threat to the security of the citizens of NATO and to international peace and stability. Terrorists and terrorist groups have continued to demonstrate their ability to cross international borders, expand their networks, enhance their capabilities and invest in new technologies to increase their reach and lethality against both NATO Allies and partners.

Delivering innovative capabilities to defeat the terrorist threat is a core pillar of NATO's efforts. Spanning technical exploitation, countering unmanned aircraft systems, biometrics, battlefield evidence and countering improvised explosive devices, NATO's work continues to address capability gaps and strengthen Allies' interoperability. It is also focused on incorporating new technologies into counter-terrorism capabilities, and ensuring through exercises that existing capabilities are fit for purpose.

Figure 3: Captured from "NATO Secretary General 2024 Report" page 15, as published in April 2025 *(Source – www.nato.int)*

1 Taken from the title of Paul Gauguin´s oil on canvas "D*'où venons-nous? Que sommes-nous? Où allons-nous?*" (Where Do We Come From? What Are We? Where Are We Going?) as painted in 1897.

... Où allons-nous ?[2]

The NATO Warfighting Capstone Concept provides five warfare development imperatives to focus and synchronize efforts to develop the Alliance military instrument of power (MIoP).

Figure 4: NATO warfare development imperatives *(Source – www.nato.int)*

One of those imperatives is **"Cognitive Superiority"** (aka 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.

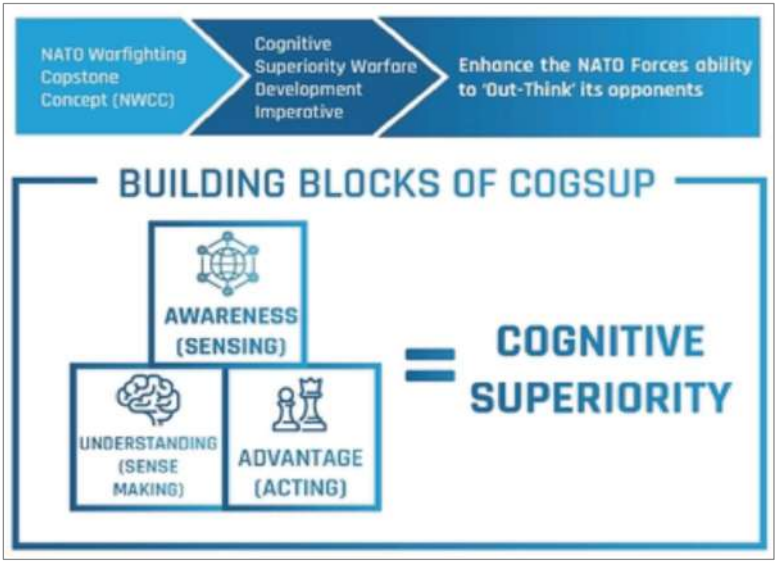


Figure 5: NATO description of Cognitive Superiority *(Source – www.nato.int)*

2 Taken from the title of Paul Gauguin´s oil on canvas "D'où venons-nous ? Que sommes-nous ? Où allons-nous ?" (Where Do We Come From? What Are We? Where Are We Going?) as painted in 1897.

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 (So Attack the Networks) remain active for achieving the Cognitive Superiority. Information collection and intelligence processing capabilities need to be reinforced, enhanced, and refined… which, in general terms, has never happened even during the Allied involvement in Afghanistan, Iraq and so on. 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 Cognitive Superiority imperative. From an Attack the Networks point of view, the current approach to Cognitive Warfare has been considered inside the essential-to-success non-lethal actions.

COGWAR integrates cyber, information, psychological, and social engineering capabilities. These activities, conducted in synchronization with other instruments of power (so not only the Military Instruments of Power (MIoP)), can affect attitudes and behaviour 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"**, so 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. Accordingly, NATO emphasizes that the resilience of each member country contributes to the overall strength and preparedness of the Alliance, but also the common cohesion and unity of effort is essential for that.

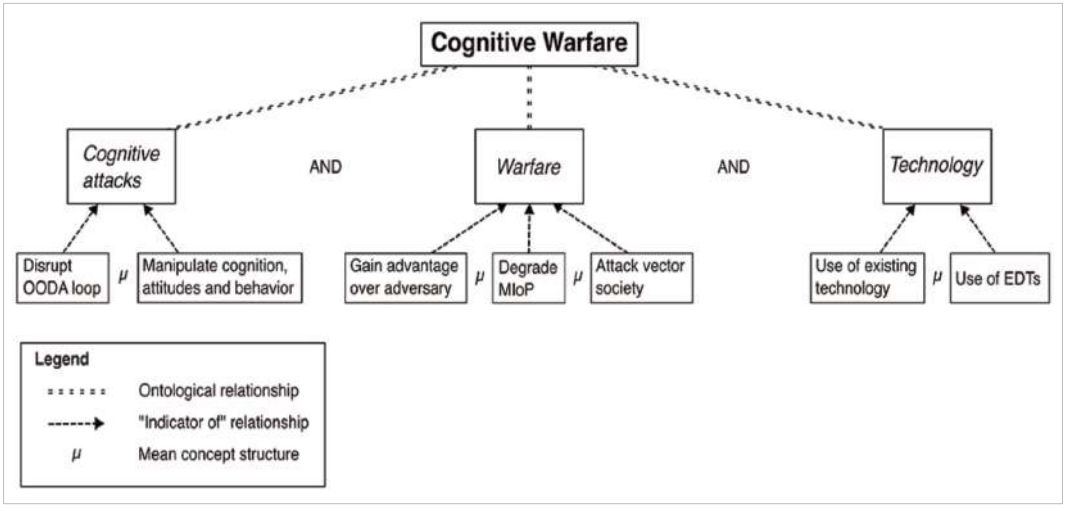


Figure 6: Visualization of NATO cognitive warfare working definition. *(Source - https://doi.org/10.3389/fdata.2024.1452129)*

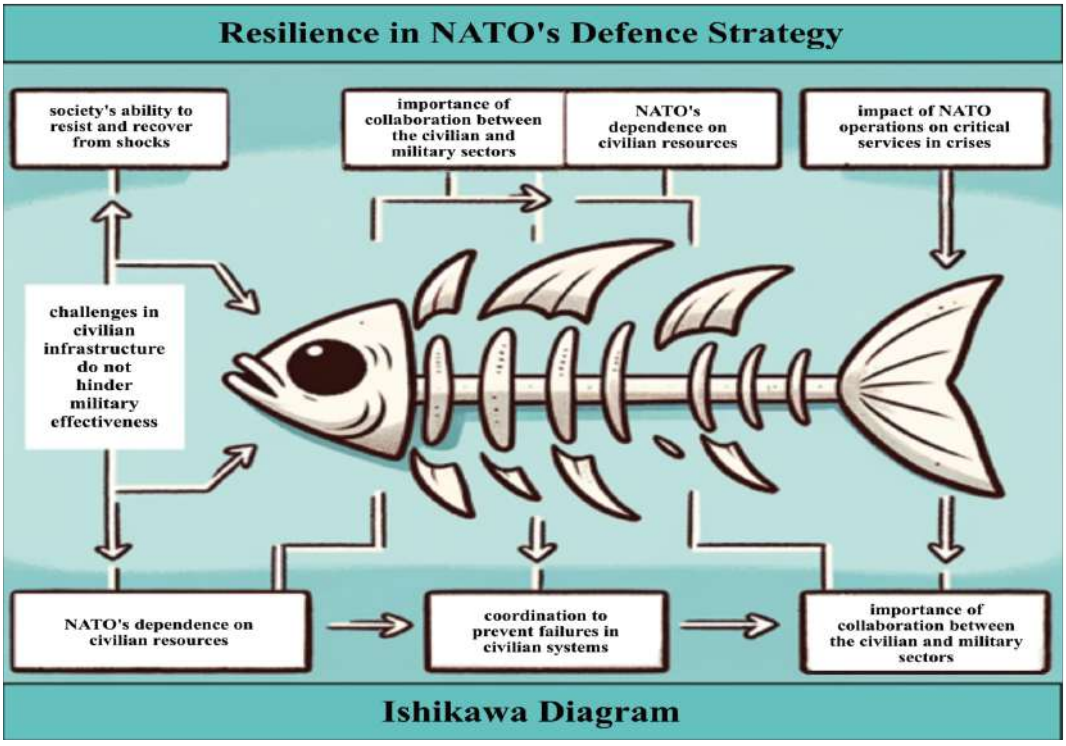


Figure 7: Structured visualization of the factors influencing resilience in the context of allied defence *(Source - www.e-arc.ro)*

Although a layered resilience is not directly related to a generic C-IED approach, it is partially applicable from 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 own actions developed in support of the achievement of positive effects over friendly human networks in benefit of strengthening own capabilities in the aim of undermining the potential development of adversary capabilities.

From the combination of the other three imperatives (**"Influence and Power Projection"**, **"Cross-Domain Command"** and **"Integrated Multi-Domain Defence"**) we arrive at the allied implementation of the concept for Multi-Domain Operations.

Multi-Domain Operations (MDO) are 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" flavor of C-IED/Attack the Networks.
- Actions over all domains and environments, which have 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 in the aim of achieving effects over the capabilities of human networks.

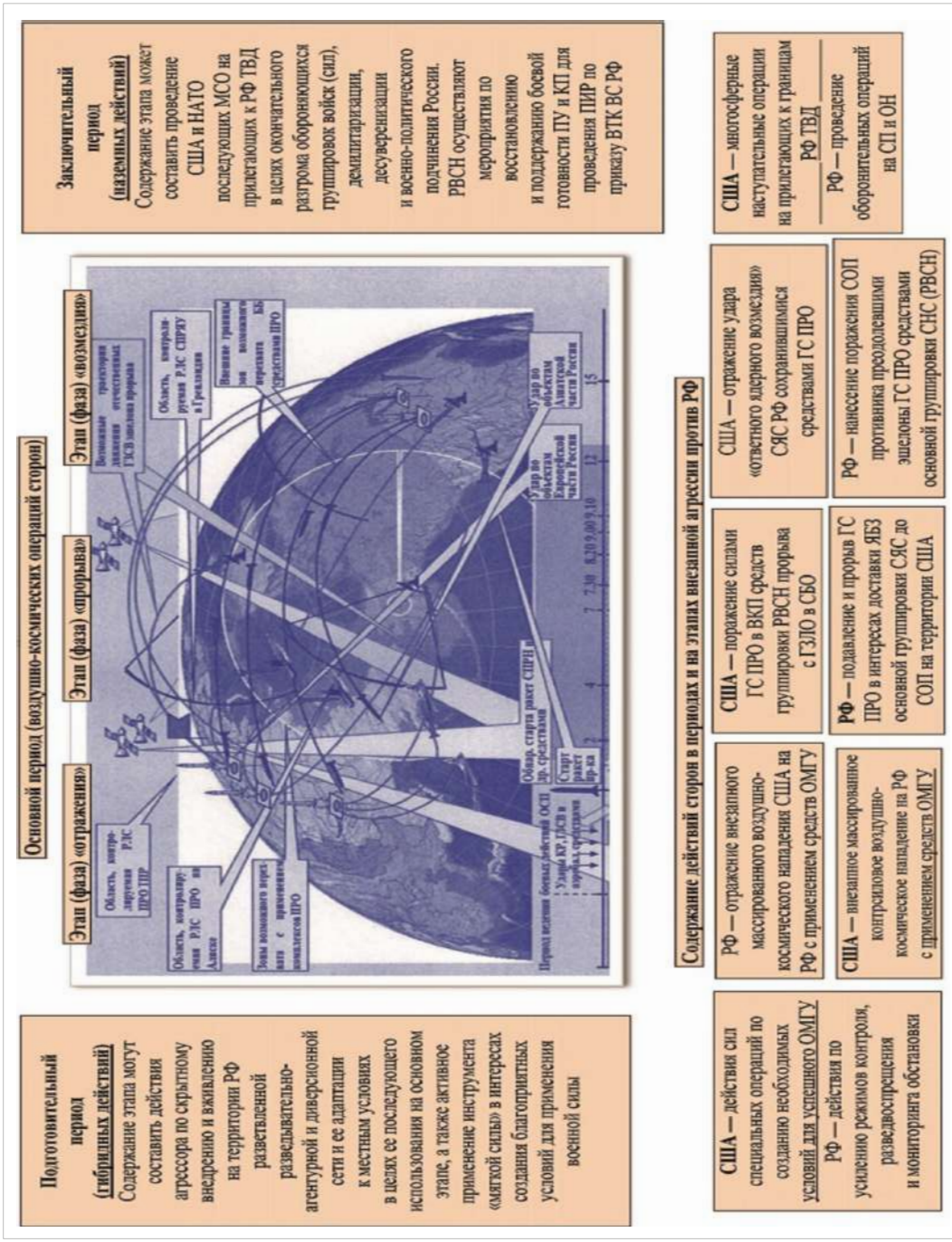


Figure 8: Russian conceptual model of bilateral interactions based on USA strategic MDO aggression *(Source - www.vm.ric.mil.ru)*

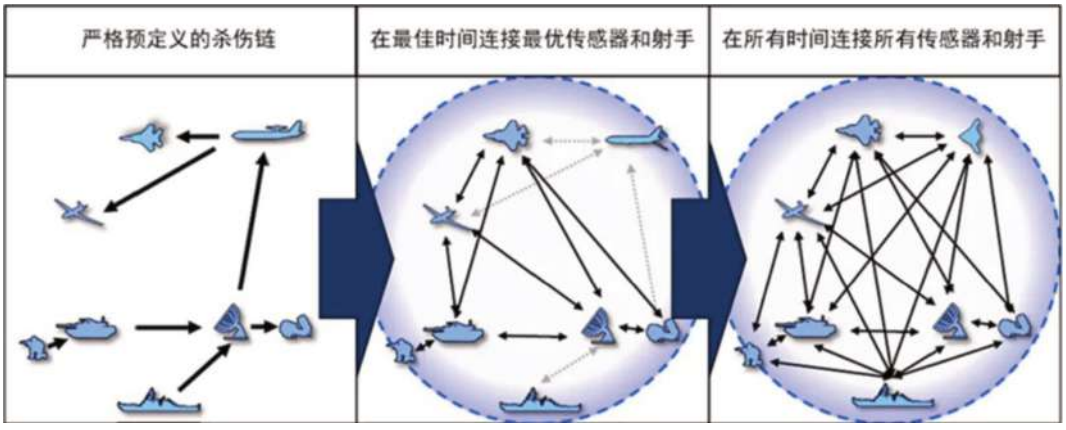


Figure 9: Joint Command & Control evolution in the sight of All-Domain Operations *(Source - www.secrss.com)*

Multi-Domain Operations is a new NATO concept... Are you really sure?

In fact, NATO Allied Command Transformation (ACT) has merely adopted concepts (Multi-Domain Extended Battlefield and Multi-Domain Operations) which were developed by the United States of America (USA) Army and Marines Corps during last decade (although finally published by the Army).

On the other hand, Russia has imitated the USA approach to MDO through their "многосферной операции, multi-sphere operations" concept.

In parallel, China adopted the equivalent to MDO "全域作战 all-domain operations" approach.

MDO finally moves around two essential elements: network-centric warfare, and deep strike capabilities as integrated at the five domains (air, land, sea, space & cyber).

If there be nothing new, but that which is! [3]

Firstly, it looks like the whole spectrum of NATO Warfare Development Agenda (WDA) is not too revolutionary in 2025.

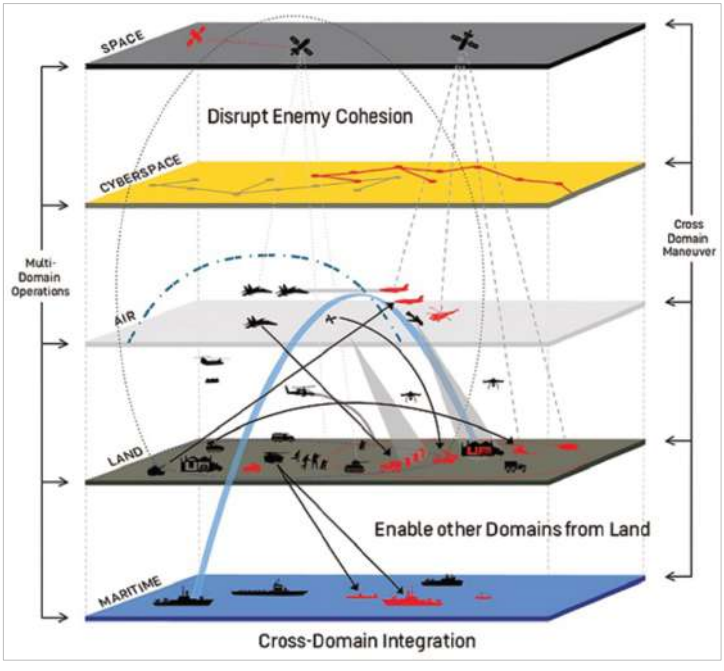


Figure 10: Cross-domain integration for Multi-Domain Operations *(Source – www.immmedia.in)*

3 From the Sonnet 59 as written by Willian Shakespeare

Secondly, it looks like the Alliance (but mostly its member nations) could currently not be ready for effectively implementing Multi-Domain Operations, due to both the NATO lack of accuracy in defining the concept and the huge effort in the development of intelligence and operations that MDO would require.

Thirdly, it seems that the MDO approach is already implemented (so fully applicable to C-IED) into the Attack the Networks approach from its very beginning of existence in 2008. Along with the evolution of the emerging threats and the persistence of IED as a future weapon of choice, that makes C-IED still valid and of course necessary. ■

"Extinction is the rule. Survival is the exception."

(Carl Sagan in his book "The Varieties of Scientific Experience: A Personal View of the Search for God", 2006)

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
- R. McDermott, "*Russian Armed Forces Test Multi-Domain Operations*", Jamestown Foundation, 9 September 2020.
- D. Solen, "*Chinese Views of All-Domain Operations*", China Aerospace Studies Institute, August 2020
- www.cssas.unap.ro
- www.secrss.com
- UK MoD Joint Concept Note 1/20 "Multi-Domain Integration" (archived)
- Ionita, Craisor *"THE CONCEPT OF MULTI-DOMAIN OPERATIONS AND ITS MULTINATIONAL UNDER-STANDING"* (STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment, 186-193) 2022

Disclaimer

This article does not represent the opinion of any national or multinational organisation; its whole content should only be considered as the opinion of the author. As all information has been obtained from open sources, potential mistakes could have been made during the research process. Please feel free to send your comments, corrections and inputs to the author; they will be highly appreciated.

ABOUT THE AUTHOR

Lieutenant Colonel Jose M Rufas graduated from the Spanish Army Military Academy in 1993. He was commissioned into the C-IED Centre of Excellence as Head of the Defeat the Device Branch in August 2016 and currently holds the post of Chief of Attack the Networks Branch. As a Military Engineer Officer, his background has been mainly based on Explosive Ordnance Disposal activities in the Spanish Army and C-IED staff issues at the multinational headquarters. In addition to his EOD Operator / EOD Officer education, he attended some other military courses regarding Parachuting, Army Staff, Information Operations, War College General/ Joint Staff, Military Search, Technical Exploitation Operations, Weapons Intelligence Team, Exploitation Laboratories, Homemade Explosives and other C-IED courses. His operational assignments include Bosnia and Herzegovina (3), Afghanistan (3), the Republic of Ecuador, Iraq and Uganda.

E-mail: jrufas@ciedcoe.org

IMPROVING UNDERWATER CAPABILITIES: THE IMPACT OF ARTIFICIAL INTELLIGENCE ON IED DETECTION AND IDENTIFICATION

By Murat Aydoğmuş, Lieutenant Commander (OF-3) TUR-N, Electronic Warfare Specialist, C-IED Centre of Excellence

INTRODUCTION

Detecting and identifying Improvised Explosive Devices (IEDs) in underwater environments presents significant operational challenges. Unlike traditional explosives, IEDs are designed in an improvised way and often activated remotely, which makes them a continuous threat in both military and civilian maritime contexts. With the increasing importance and reliance on naval and offshore infrastructure for trade, energy production, and defense, the risk posed by the underwater threat has become a critical concern for global security. More recent incidents, such as the detonation of limpet mines illustrate the significant risks posed by explosives that can be manufactured with relative ease and evolve into asymmetric threats[1].

Detecting IEDs and other potentially suspicious underwater objects represents a critical component of operations. These threats present significant risks not only to naval and commercial assets but also to human life. Ensuring the safe identification and handling of such underwater hazards is therefore of great importance. Traditional detection methods, such as sonar scanning and manual diver inspections, have proven time-consuming, labor-intensive, and risky, particularly in deep-sea environments or areas with poor visibility. Advancements in artificial intelligence (AI) have revolutionized the field of underwater threat detection. Tools developed with AI support have improved the precision and effectiveness of detecting underwater objects[2]. Deep learning models trained on extensive sonar and optical image datasets can quickly identify possible threats, minimize false alarms, and enhance overall situational awareness. Additionally, Autonomous Underwater Vehicles (AUVs) equipped with AI-driven navigation and object recognition capabilities can autonomously patrol high-risk areas, minimizing the need for human divers and enhancing operational safety. Research efforts around the world have focused on developing AI-supported sonar processing to improve detection capabilities in complex marine environments[3].

As underwater threats continue to evolve, the integration of AI solutions remains an important aspect of modern naval defense and maritime security. This article examines the technological advancements in AI-aided detection and identification of small underwater targets or threats with an emphasis on IEDs, highlighting the benefits, challenges, and future potential of these systems[3].

TRADITIONAL METHODS

To detect and classify underwater IEDs or potential suspicious objects, there are some traditional approaches like using sonar scanning and analysing the screen, magnetic anomaly detection (MAD), diver-based inspections, and remotely operated vehicles (ROVs). The primary technology used for underwater detection is sonar systems. Sonar devices rely on sound waves to detect objects or threats underwater because electromagnetic waves are heavily absorbed and attenuated by water, making them ineffective for communication or detection.

Sonar devices have different monitoring technology according to the system's active or passive operation mode. While passive systems are used to listen to the environment without any emissions, active systems send out pulses and receive the reflections. In this article, examples will be given from active and high-resolution sonar systems. Although there are different kinds of sonar systems used for underwater monitoring like multi-beam echo sounders, forward-looking sonar, side-scan sonar (SSS), and synthetic aperture sonar (SAS) systems, the use of SSS and SAS operation will be briefly explained in this article. Both sonar systems provide detailed images of the underwater environment.

Magnetic anomaly detection (MAD), on the other hand, identifies changes in the Earth's magnetic field caused by metallic objects, and these systems are used traditionally to detect anomalies and potential underwater targets[4]. While MAD is particularly useful for detecting metal-based threats, it is less effective when it comes to non-metallic IEDs.

Sonar System Operations:

The underwater environment poses many challenges because of the complex characteristics of water. Several sonar technologies are used for seabed scanning and small object detection, and these systems typically operate at higher frequencies, which allows for high-resolution imaging.

In the traditional approach, detecting small objects relies heavily on manual analysis of sonar images, a process that is time-consuming and highly dependent on the skill of the operator. This dependence can lead to inconsistent outcomes and limits scalability, particularly when large amounts of data need to be processed. The inherent complexity of the underwater environment adds an additional layer of difficulty to detection operations[5]. Factors such as noise, clutter, and varying seabed conditions make it difficult for operators to accurately identify objects manually.

a. Side Scan Sonar (SSS):

SSS is an important tool for detecting underwater objects, including IEDs and other small objects on the seabed. SSS works by emitting conical or fan-shaped pulses that are directed downward toward the seabed at a wide angle, perpendicular to the sensor's path through the water. The sensor can be towed behind a surface vessel or submarine, or it can be mounted on the ship's or unmanned vehicle's hull for more stationary scanning.

The sonar emits sound waves, which interact with the seafloor and any objects resting on or buried within it. These sound waves reflect to the sonar system, and the intensity of these acoustic reflections is recorded. The resulting data is captured in a series of cross-track slices, which can then be analyzed to reveal anomalies on the seafloor.

This sonar is useful for detecting metallic objects like underwater mines, IEDs, and debris, as these typically produce strong acoustic reflections. However, side-scan sonar can also detect non-metallic objects when their shape and density exhibit significant contrast relative to the surrounding environment. For example, irregularities caused by buried objects or disruptions in the seafloor structure might indicate the presence of IEDs, which are often buried or camouflaged[6].

b. Synthetic Aperture Sonar (SAS):

SAS is also a powerful tool for obtaining high-resolution underwater images and they can also be used for detecting the objects like mines, underwater IEDs or other potential objects. SAS, which is mounted on a UUV, moves along a track and synthesizes a much larger virtual array from many pings. It

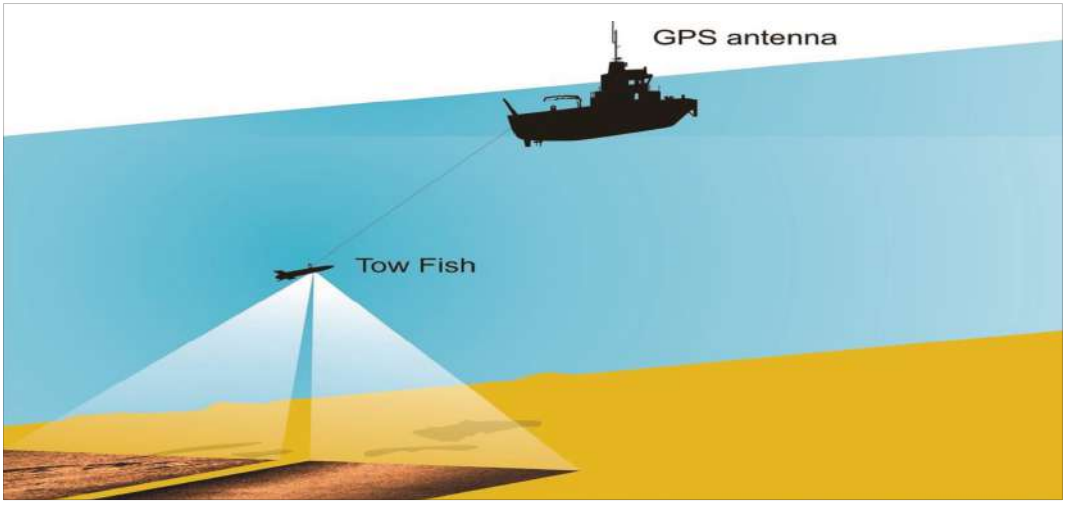


Figure 1: Illustration of SSS Operation[7]

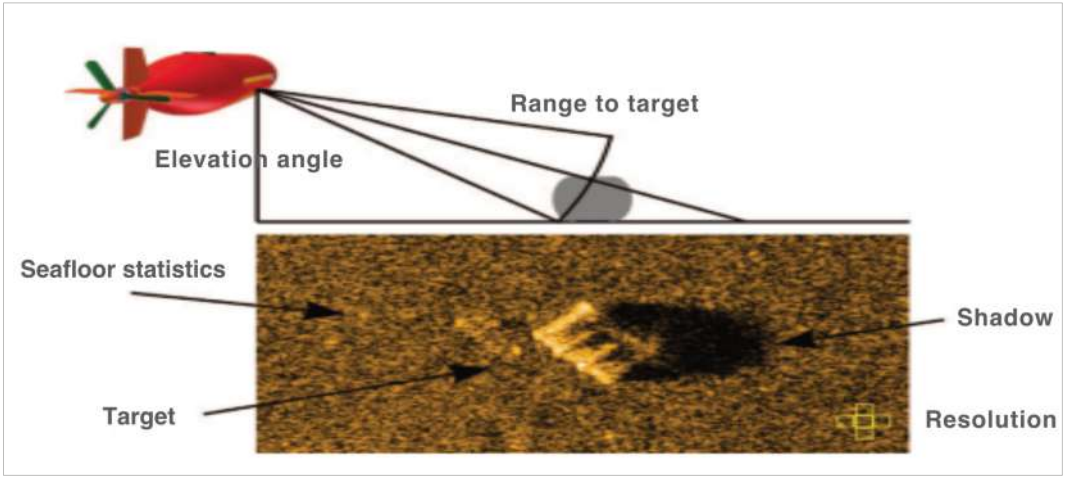


Figure 2: Illustration of SAS Operation[8]

continuously records backscattered signals from the seafloor or the objects. The system coherently combines the echoes received at different positions, effectively synthesizing a large aperture. Much finer resolution is obtained with SAS[8].

Regarding the detection of IEDs or small buried objects underwater; they offer more detailed imagery of the seafloor and large areas are scanned efficiently with high-resolution outputs.

Magnetic Anomaly Detection (MAD) Operations:

MAD systems utilize sensitive magnetometers designed to detect perturbations in the Earth's magnetic field induced by the presence of ferrous objects[9]. Normally, the Earth's magnetic field is quite stable, and natural underwater materials like sand or water don't affect it much. But when there is a metal object – like a mine casing or parts of an IED – it might create a small disturbance in the magnetic field.

MAD sensors are used to detect these disturbances, known as magnetic anomalies. MAD sensors can be attached to ships, underwater drones, or even aircraft flying low over shallow waters. As the sensor moves, it constantly measures the magnetic field. If it detects an unusual magnetic signal, it marks that location as a potential threat. This is especially useful when IEDs are made with metal parts, and MAD can help find them even if they are buried under the seabed or not visible on sonar images. That's one of the biggest strengths of MAD – it can detect hidden objects in cluttered underwater environments.

However, while MAD is great for detecting where a metallic object might be, it doesn't tell us what the object is. A rock anchor, an old pipe, or a mine might all produce similar magnetic signals. So, once MAD finds something suspicious, other tools like sonar, cameras, or divers are usually needed to take a closer look and identify the object. The greatest limitations are that small devices have a weaker magnetic footprint, MAD only works effectively at close range, and small anomalies are only noticeable when background magnetic noise is low.

AI SUPPORT IN UNDERWATER MONITORING

In the traditional approach, operators visually inspect the high-resolution sonar imagery, and they look for shapes, shadows, textures, and other cues to identify potential threats like IEDs or mines, which is very dependent on experience and familiarity with underwater environments.

In the field of underwater target detection and identification, AI offers a transformative alternative to traditional methods by enabling automated processes that reduce or minimize human intervention. Unlike traditional approaches – which often rely on manual analysis, and an operator-dependent decision-making– AI-based systems utilize data-driven models to autonomously detect and identify underwater objects. This shift is particularly significant when considering the complex and dynamic nature of the underwater environment, where factors such as light absorption, turbidity, background clutter, and noise substantially hinder image clarity and object visibility.

The effectiveness of AI in such scenarios is heavily dependent on the quality of the input data. Obtaining high-resolution, noise-free imagery is essential for accurate detection and reliable identification. However, due to environmental constraints, such ideal conditions are not always achievable. Therefore, during the algorithm development phase, preprocessing tech-niques such as denoising, contrast enhancement, and super-resolution play a critical role in preparing the data for subsequent analysis. These preprocessing steps not only improve the visual quality of the images but also enhance the performance of AI models by ensuring that essential features are preserved and emphasized.

In addition, the variety and richness of a dataset have a direct impact on how robust and generalizable the trained models are. When a dataset covers diverse object appearances, angles, environmental scenarios, and sensor types, it allows AI systems to learn more detailed and representative features. As a result, this enhances detection performance and lowers the chances of false alarms or missed detections.

In recent years, there has been increasing interest in utilizing deep learning approaches – like convolutional neural networks (CNNs) and transformer-based models – for automatically detecting and classifying objects in underwater environments. These techniques have demonstrated strong potential in recognizing patterns and irregularities that might be challenging for human observers to detect. Even though IEDs are typically non-standard in shape and composition since they are constructed using improvised and unpredictable methods, AI-based approaches can still provide valuable insights. While they may not always deliver definitive identification, they are highly effective in flagging potential threats and drawing the operator's attention to regions of interest.

Ultimately, the integration of AI into underwater detection systems enhances situational awareness, operational efficiency, and decision-making capabilities. By combining high-quality data acquisition, advanced preprocessing techniques, and powerful AI algorithms, it becomes possible to

develop robust systems capable of performing in real-time, even under challenging conditions. This not only increases the safety of underwater operations but also reduces the cognitive load on human operators, enabling more focused and informed assessments of suspicious objects.

Although this article does not aim to explore the technical background in depth, it is important to highlight that significant research has been dedicated to the automatic detection of underwater objects. These studies span a broad methodological spectrum, encompassing single-stage detection models, two-stage detection frameworks, and more sophisticated multi-stage systems.

Single-stage methods integrate object localization and classification into a unified pipeline, enabling rapid inference and making them particularly advantageous for real-time applications and resource-constrained, modular systems. Conversely, two-stage and multi-stage approaches introduce intermediate processing steps – such as region proposal, candidate filtering, and refined classification – that, while computationally more demanding, often yield higher detection precision and robustness, especially in complex or visually cluttered underwater environments[10].

Various algorithms have been developed within each of these methodological categories, and the research community continues to explore novel techniques and architectures in pursuit of improved performance. These efforts reflect the intrinsic challenges posed by the underwater domain, where visibility limitations, sensor noise, and the irregular, non-standardized construction of IEDs complicate reliable identification. As such, there is no single superior approach; rather, each method offers context-specific advantages, and their relative effectiveness is often determined by operational constraints such as processing time, hardware capabilities, and mission-critical requirements.

In this context, the ongoing development of AI-driven detection systems is of particular significance. Even when definitive classification of an object as an IED is not immediately possible, the ability to automatically flag anomalous or suspicious items contributes substantially to enhancing operator situational awareness and facilitating more focused human analysis. Therefore, the quality, speed, and adaptability of the detection algorithms play a crucial role in the overall efficacy of underwater surveillance and security operations.

Among more recent approaches, the integration of advanced payload systems on unmanned underwater vehicles (UUVs) has significantly enhanced target detection capabilities. These platforms are increasingly equipped with both optical and sonar imaging technologies[11], enabling the collection of comple-mentary data sets. By applying multi-modal data fusion techniques – where optical imagery provides high-resolution detail and sonar imaging offers greater penetration in turbid or low-visibility environments, the overall accuracy and reliability of underwater detection systems can be substantially improved.

This synergistic use of sensor modalities allows for a more robust assessment of submerged objects, particularly in complex and dynamic underwater conditions. As a result, such technological advancements contribute to safer and more effective operations, whether in military reconnaissance or counter-IED missions.

As an example, limpet mines used as underwater IEDs are typically rudimentary and constructed with readily available materials, making them difficult to detect or defend against. The improvised nature of these devices means that they may lack the sophisticated triggering mechanisms of standard military mines, but this also makes it harder to trace and neutralize[12]. These mines may be manually placed by divers or deployed using UUVs, making their detection and identification a challenge. The use of AI-driven systems to detect and identify such underwater IEDs, including limpet mines, by utilizing advanced sonar imaging and optical technologies is a very good application area. As it was stated, when fused together, these techniques offer greater accuracy in distinguishing between benign objects and potential threats, contributing to safer operations in naval environments.

CONCLUSION

In recent years, there have been many research topics concentrated on leveraging AI-supported systems for underwater object detection. The primary goal of these studies is to improve situational awareness and ensure safer operations by minimizing the need for human intervention in risky underwater environments. The effectiveness of these automated detection systems heavily depends on the volume and diversity of the training data, as richer and higher-quality datasets allow AI models to perform more reliably across different environments and object variations.

Although the improvised nature of IEDs – characterized by their unpredictable shapes, materials, and deployment methods – poses significant challenges for reliable identification, the application of AI-supported tools plays a critical role in drawing attention to potential underwater threats. Ultimately, minimizing human exposure while maximizing detection reliability through automated systems not only improves safety but also strengthens the overall effectiveness of underwater threat mitigation strategies. ■

REFERENCES

1 The Maritime Executive, "Ambrey: Tanker at Ust-Luga May Have Been Hit With Limpet Mines," The Maritime Executive, Feb. 12, 2025. [Online]. Available: https://maritime-executive.com/article/ambrey-tanker-at-ust-luga-may-have-been-hit-with-limpet-mines

2 M. Kanguya, "Smart Oceans: The Rise of AI in Deep-Sea Exploration," The Future List, Feb. 2025. [Online]. Available: https://www.thefuturelist.com/smart-oceans-the-rise-of-ai-in-deep-sea-exploration/

3 M. Aubard, A. Madureira, L. Teixeira, and J. Pinto, "Sonar-based Deep Learning in Underwater Robotics: Overview, Robustness and Challenges," arXiv preprint arXiv:2412.11840, 2024. [Online]. Available: https://arxiv.org/abs/2412.11840

4 Clem, T.; Allen, G.; Bono, J.; McDonald, R.J.; Overway, D.; Sulzberge, G.; Kumarb, S.; King, D. Magnetic sensors for buried minehunting from small unmanned underwater vehicles. In Proceedings of the Oceans'04 MTS/IEEE Techno-Ocean '04 (IEEE Cat. No.04CH37600), Kobe, Japan, 9–12 November 2004; Volume 2, pp. 902–910.

5 F. Zhao, B. Huang, J. Wang, X. Shao, Q. Wu, D. Xi, Y. Liu, Y. Chen, G. Zhang, Z. Ren, J. Chen, and K. Mizuno, "Seafloor debris detection using underwater images and deep learning-driven image restoration: A case study from Koh Tao, Thailand," Marine Pollution Bulletin, vol. 214, 117710, 2025. [Online]. Available: https://doi.org/10.1016/j.marpolbul.2025.117710

6 NOAA Ocean Exploration, "Exploration Tools: Side-Scan Sonar," NOAA Ocean Explorer. [Online]. Available: https://oceanexplorer.noaa.gov/technology/sonar/side-scan.html [Accessed: Mar. 24, 2025].

7 Robert Wilson Marine Technologies (RWMT), "Side-Scan Sonar," RWMT Surveying Tools. [Online]. Available: https://www.rwmt.se/surveying-tools/side-scan-sonar. [Accessed: Mar. 24, 2025].

8 R. Edgar, "Introduction to Synthetic Aperture Sonar," in Sonar Systems, InTechOpen, 2011. [Online]. Available: https://cdn.intechopen.com/pdfs/18868/InTech-Introduction_to_synthetic_aperture_sonar.pdf

9 CAE, "Magnetic Anomaly Detection Extended Role (MAD-XR)," CAE, Mar. 2023. [Online]. Available: https://www.cae.com/media/media-center/documents/datasheet.MAD-XR.pdf

10 SharkYun, "Computer Vision — Object Detection, One-Stage vs Two-Stage," Medium, Oct. 31, 2024. [Online]. Available: https://sharkyun.medium.com/computer-vision-object-detection-one-stage-vs-two-stage-b05dbff88195

11 Kim, H.-G.; Seo, J.; Kim, S.M. Underwater Optical-Sonar Image Fusion Systems. Sensors 2022, 22, 8445. https://doi.org/10.3390/s22218445.

12 J. D. Caverley, "From the Editors," Naval War College Review, vol. 77, no. 3, pp. 1–2, Summer/Autumn 2024. [Online]. Available: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1756&context=nwc-review

ABOUT THE AUTHOR

Lieutenant Commander Murat Aydoğmuş was commissioned into the C-IED Centre of Excellence as a C2 Electronic Warfare Specialist in the Defeat the Device Branch in August 2023. After assuming this position, he organized the 6th NATO C-IED Technology Workshop in Seville, Spain, in 2024. He holds master's degree in Electrical Engineering and Engineering Acoustics from the Naval Postgraduate School. His background is primarily based on maritime projects and research and development activities in the maritime domain. He is currently pursuing PhD studies in underwater target detection using modern deep-learning models.

Email: maydogmus@ciedcoe.org

INFRASTRUCTURE AND COMMERCIAL PROJECTS: EO CLEARANCE AND RISK MANAGEMENT

By Dr Robert Keeley, RK Consulting (EOD) Ltd

INTRODUCTION

International Mine Action Standards (IMAS) have become the benchmark for humanitarian mine action since they were first introduced nearly a quarter of a century ago. Yet they don't fit exactly into commercial clearance work.

The aim of this paper is to explore the differences between humanitarian and commercial perspectives, how they both influence attitudes to the clearance of commercial projects and infrastructure. The paper also makes recommendations on best practice for EO risk management on infrastructure and commercial projects, drawing on the relevant elements of IMAS where possible.

THE HUMANITARIAN PERSPECTIVE

It may be useful to start with a definition of 'humanitarian'. For this it is possible to refer to two different United Nations (UN) General Assembly resolutions, namely:

- 46/182 (19 Dec 1991)
- 58/114 (5 Feb 2004)

These describe humanitarian action as having four principles, which are:

- Neutrality
- Humanity
- Impartiality
- Independence (added 2004)

The principles have been defined in an elaboration by the UN Office for the Coordination of Humanitarian Affairs (OCHA)[1], as set out in **Table 1** below.

Ser	Item	Table Heading	Remarks
(a)	(b)	(c)	(d)
1	**Humanity**	Human suffering must be addressed whenever it is found. The purpose of humanitarian action is to protect life and health and ensure respect for human beings.	"wherever it is found"
2	**Neutrality**	Humanitarian actors must not take sides in hostilities or engage in controversies of a political, racial, religious or ideological nature.	
3	**Impartiality**	Humanitarian action must be carried out on the basis of need alone, giving priority to the most urgent cases of distress and making no distinctions on the basis of nationality, race, gender, religious belief, class or political opinions	"On the basis of need alone"
4	**Independence**	Humanitarian action must be autonomous from the political, economic, military or other objectives that any actors may hold with regard to areas where humanitarian action is being implemented	"Humanitarian action must be autonomous from… economic… objectives"

Table 1. OCHA elaboration on humanitarian action.

1 Source: OCHA on Message: Humanitarian Principles, November 2011
https://www.unocha.org/sites/unocha/files/dms/Documents/v.2.%20website%20overview%20tab%20link%202%20Humanitarian%20Principles.pdf

When one also takes into account the language of the 1997 Anti-Personnel Landmine Ban Convention (APMBC), and the 2008 Convention on Cluster Munitions (CCM), there is a clear requirement to clear ***all*** contamination. For example, CCM says in Article 4:

> *"Each State Party undertakes to clear and destroy, or ensure the clearance and destruction of, cluster munition remnants located in cluster munition contaminated areas under its jurisdiction or control… not later than ten years from [its entry into force}.*

It is generally accepted that the only limitation on humanitarian mine action is the availability of funding. Much of the focus of humanitarian mine action has therefore been on fundraising. However, this imperative to clear all contamination does not apply to commercial projects, which, by their very nature, will only be interested in clearing contamination relevant to their activities.

THE COMMERCIAL PERSPECTIVE

Definitions

When exploring the commercial perspective, it is worth defining non-profit and for-profit organisations. These definitions, from the United States Chamber of Commerce[2], are set out in **Box 1** below.

- **Non-profit organisations.** A non-profit organisation has a legally approved purpose or social cause beyond profit generation. The organisation's income is not dispersed to any shareholders but instead is invested back into the organisation.
- **For-profit organisations.** A for-profit company is an organisation that exists to earn a profit. These entities do not have legal obligations dictating where their profit goes. Instead, they can disperse the funds among the owners and employees or spend it however they choose.

Box 1. Definitions of non-profit and for-profit organisations.

It should also be remembered that non-profit and for-profit organisations are likely to have different tax obligations, depending on (a) where they are registered and (b) where they are working.

There are three other useful concepts that are usefully defined here. These are 'infrastructure'[3] and the economic concepts of 'public good'[4] and 'market failure'[5]. These are defined in **Box 2** below.

- **Infrastructure.** The basic systems and services, such as transport and power supplies, that a country or organisation uses in order to work effectively.
- **Public good.** A public good can be defined as a commodity or service that is provided without profit to all members of a society, either by the government or by a private individual or organisation.
- **Market failure.** A situation in which a market does not operate as it should, for example where the supply of a product is not related to the level of demand for it.

Box 2. Definitions of infrastructure, public good and market failure.

Economic perspective on mine action

Taking all of these definitions together, humanitarian mine action can be described as a form of market failure, as it is a product where the intended beneficiary is not the customer. Not least because most beneficiaries could not afford to meet the full cost of the services. Commercial mine action activities, on the other hand, have a conventional buyer-seller relationship. These two models are represented graphically in **Figure 1** below. Infrastructure projects may be public goods as defined in **Box 2** above, but, as will be discussed below, they should be regarded in the same light as commercial projects in that they require focused, project-oriented action rather than the clearance of all EO contamination.

2 https://www.uschamber.com/co/start/strategy/nonprofit-vs-not-for-profit-vs-for-profit
3 https://dictionary.cambridge.org/dictionary/english/infrastructure#google_vignette
4 Source: https://languages.oup.com/google-dictionary-en/
5 https://dictionary.cambridge.org/dictionary/english/market-failure

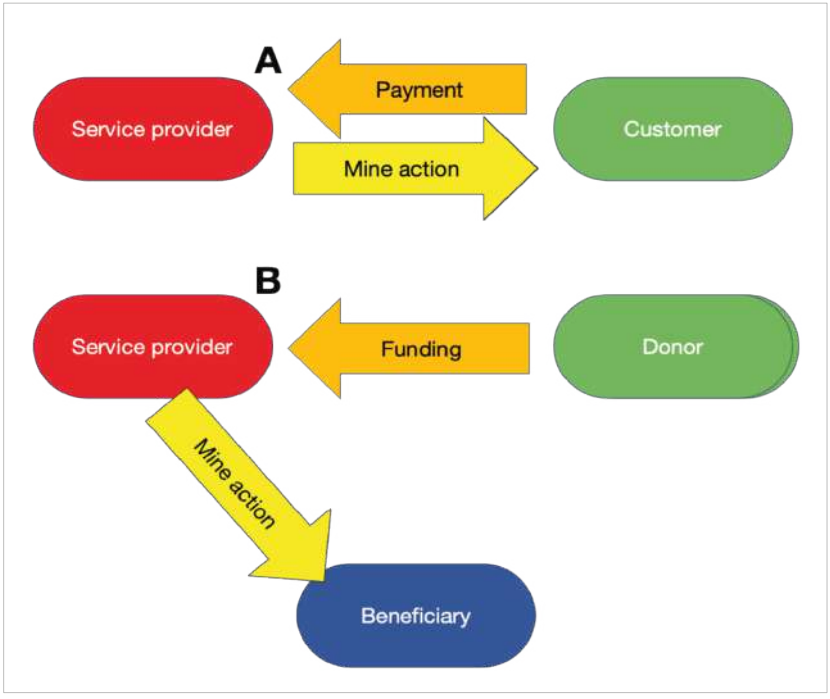


Figure 1. Behaviour of the market in (A) commercial or (B) humanitarian mine action.

Therefore, using these definitions, there is no objective reason why commercial mine clearance organisations cannot undertake humanitarian clearance projects, or indeed why mine action NGO should not bid on commercial projects. Both types of organisation will have different legal and tax liabilities of course, but those are beyond the scope of this paper. Some thoughts on how NGO should treat their pricing of commercial or infrastructure bids are nevertheless set out in **Table 2** below.

Ser	Ownership	Definition	Suggested	Remarks
(a)	(b)	(c)	(d)	(e)
1	Household	Land needed by households for subsistence and livelihoods	Direct from project funds, at no charge to beneficiaries	Up to 2 Ha per household[1]
2	Community	Village schools, ponds, wells, etc		
3	State-owned infrastructure	Publicly owned infrastructure (such as road networks) which have their own maintenance and refurbishment budgets	NGO does the work on a cost recovery basis, charged to the infrastructure project, within overall priority setting process and program scope	Costs calculated using the NGO's standard budgeting processes
4	Commercial	Privately-owned land or facilities (beyond those covered by Ser 1) where the profit from operation is held by the owners.	The NGO will do the work on a cost + (perhaps 10%) basis. Profits treated as per legal requirement in country of incorporation.	For large projects (over $100,000), it is recommended that separate teams not funded by humanitarian budgets should be used. Larger commercial projects may also need approval by the NGO board.

Notes:

1. This figure is from standard World Bank estimates of the land needed by rural households in South-East Asia. This figure may vary depending on the carrying capacity of land in other countries. However, this figure should be used unless alternative planning data is available.

Table 2. NGO clearance of infrastructure or private land: possible pricing arrangements

Economic perspectives on project management

Commercial and infrastructure projects, whether they be private or public sector, are governed to a very large degree by the return they will bring on their initial investment. This return is measured by a number of economic concepts including:

- The discount rate
- Internal rate of return (IRR)
- Net Present Value (NPV)

Brief definitions[6] of these are given in **Box 3** below.

- **Discount rate**: a rate of interest that you use to calculate the present value of an amount of money that you receive or pay in the future.
- **Internal rate of return**: the average amount of money earned each year from a particular investment, calculated by comparing how much money it makes each year with the original amount invested.
- **Net present value**: The present value of an investment's future net cash flow (= difference between the money coming in and going out) after the cost of the original investment has been subtracted.

Box 3. Economic terms used in project management.

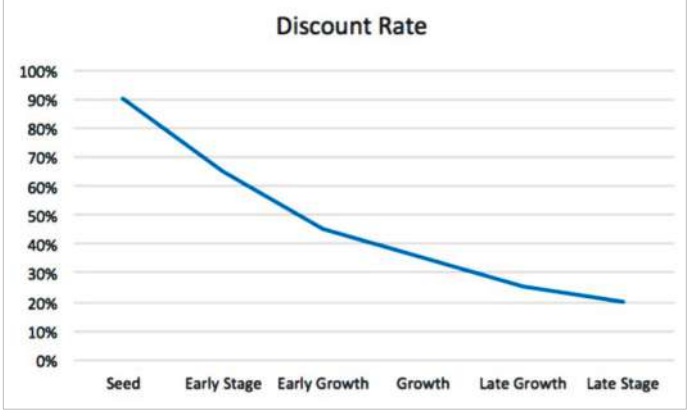


Figure 2. An example of the effect of discounting on the future value of money.

The key points from these definitions are that (a) costs paid for using today's money and (b) today's money is worth less than tomorrow's money. Furthermore, because clearance is typically a preliminary activity it is particularly expensive. A graphical representation[7] of the decreasing value of money over time is shown at **Figure 2**.

Thus, any demand by commercial projects will depend on their exposure to risk. This is discussed in more detail below.

A formal definition of risk

People often use the terms 'risk', hazard' and 'threat' interchangeably. However, risk is a mathematical concept and as such has a formal definition. IMAS 04.10[8] gives a version of that definition, which it takes from ISO Guide 51:1999:

> *A "combination of the probability of occurrence of harm and the severity of that harm".*

Expressed formally, this takes the following form:

$$R = f(i_p, o_s)$$

Where R = risk, ip is the probability of the incidence and Os is the severity of the outcome. Practically speaking, risk can also be considered a function of hazard plus activity: it doesn't matter how contaminated an area is if nobody goes there (from a risk perspective).

This can be used in something called an 'expected monetary value' (EMV) calculation which can be used to compare the cost of taking a precaution with the potential cost of an outcome should that precaution not be taken. Use of an EMV calculation is explained in more detail in International Ammunition Technical Guidelines (IATG) 02.10[9] Para 15.1.

6 https://dictionary.cambridge.org/
7 https://www.finyear.com/On-Investors-and-Discount-Rates_a35557.html
8 https://www.mineactionstandards.org/standards/04-10/
9 https://data.unsaferguard.org/iatg/en/IATG-02.10-Introduction-risk-management-IATG-V.3.pdf

Attitudes to risk

Risk calculations help determine a project's exposure to risk. However, they do not fully explain people's (or institutions') attitudes to risk. These generally range from risk-averse to risk seeker, but on many occasions the commercial mine action service provider encounters clients who are tolerant of the potential risk from EO contamination. **Figure 3** sets out a graphical representation of the spectrum of different attitudes to risk[10].

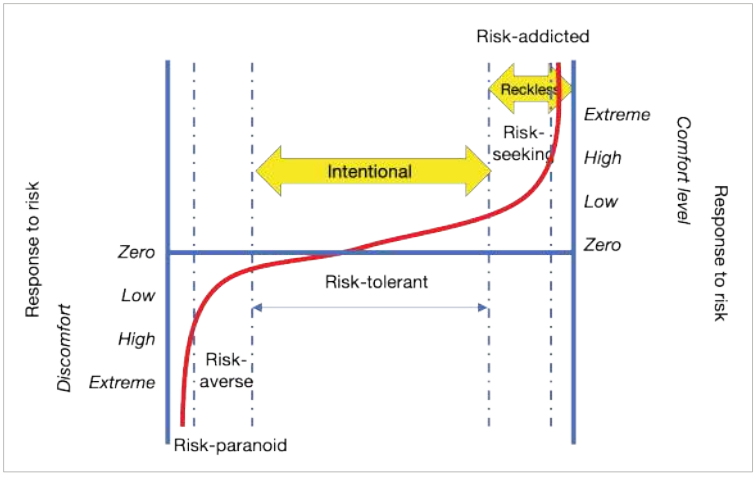


Figure 3. The spectrum of different attitudes to risk.

Incidentally, those familiar with the provision of explosive ordnance risk education (EORE) will recognise where the two categories of risk-taking behaviour[11] (the intentional and the reckless) fit on this spectrum.

It may seem strange to outsiders that any commercial project could be tolerant of a risk from EO. The principles behind project finance and EMV go some way to explain that. Mine action is an expensive, up-front activity to manage a hazard (EO) that may not actually impact the project and may not actually even be present. However, there is another dimension, which is that EO poses different types of risk, not all of which act in the same direction. This is best explained using the 'Bow Tie' risk management tool[12], as set out in **Figure 4.**

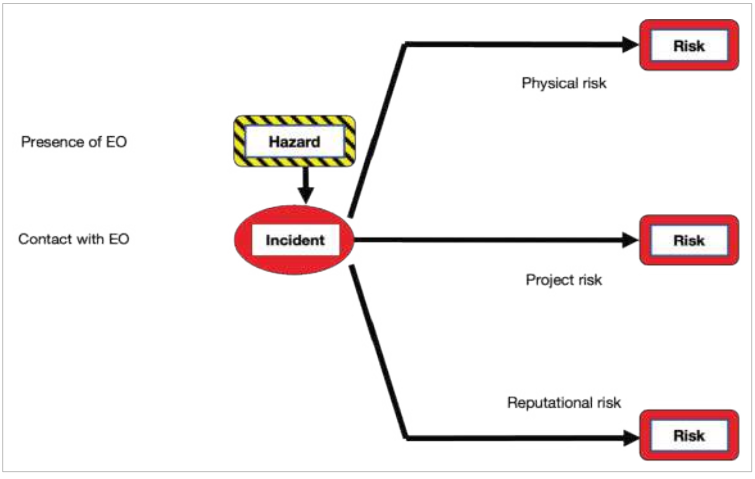


Figure 4. Assembling the EO risk bowtie (1). Identifying the potential consequences.

In a 'bow tie' risk diagram everything starts at the centre with the hazard and the incident. IMAS 04.10 also gives a useful definition of hazard, which it also takes from ISO Guide 51:1999:

A "potential source of harm".

It also defines incident thus:

"an event that gives rise to an accident or has the potential to lead to an accident".

10 https://www.managementyogi.com/2022/04/risk-attitude-and-risk-attitude-spectrum.html
11 First set out in a UNICEF handbook in 2005.
12 https://www.gov.uk/government/news/bowtie-a-visual-tool-to-keep-an-overview-of-risk-management-practices

In this context, the hazard is the (potential) presence of EO and the incident is an incident arising from contact with that EO. At first it is only necessary to set out the right-hand side of the 'bow tie', namely the consequences. The left-hand side can be completed later. These can be separated into three different potential consequences, which are defined below:

- **Physical risk.** Death, injury or damage to property or equipment arising from an EO incident.
- **Project risk**. Delays or additional costs arising from an EO incident
- **Reputational risk**. The damage to a project or a project implementer's reputation amongst relevant stakeholders, arising from an EO incident, with potential to affect future engagement (such as the allocation of future funding or the awarding of subsequent contracts).

Whereas both physical and reputational risk would tend to make a project more risk averse, project risk (as defined here) has the potential to pull in both directions. Project managers must decide on the balance of risk between the cost of preventative action and the potential cost of an incident and for unplanned delays. This is exacerbated by the higher cost of preliminary activities as described in the discussions on discounting above. The potential implication of this need to balance risks is illustrated in the case study described in **Box 4** below.

An international pharmaceutical company was considering undertaking an organic medicinal plant agribusiness project in a country in South-East Asia. Their representatives had heard about the potential risk of EO contamination (the planned project site was in the general area of the former Ho Chi Minh Trail) and they approached a commercial demining company for advice.

The commercial demining company gave a quote for full clearance of the entire site. The quoted cost for the clearance meant that the agribusiness project would no longer be profitable and the project did not proceed.

Box 4. A real case study of the effect of EO clearance costs on a commercial project.

The example as set out in **Box 4** above a critical thing about clearance of commercial projects (or infrastructure). Unlike humanitarian projects – especially ones focussed on compliance with the two conventions – clearance per se is not the focus; rather, EO clearance is an enabler to allow the wider goals of the project to be achieved in a safe and timely manner. The focus of EO-related activities on this wider project Schwerpunkt will be discussed in more detail in the section on 'scope of works' below.

One final point that should be introduced here is the question of liability. This is not the place to discuss the legal aspects of risk and in any event a project's legal exposure will vary depending on the relevant national laws. But in general, it is reasonable to say that both physical risk and reputational risk will enter into considerations of liability.

Managing risk

The perspective of the mine action sector on the management of risk is set out in IMAS 07.14. However, it is suggested that this is largely seen through the humanitarian lens.

Mine action practitioners will recognise that the commercial demining company described in **Box 4** presented a false dichotomy to their potential client. Full clearance was not the only option available. A risk management approach could have been taken. Before this risk management approach is discussed it is necessary again to introduce some definitions, drawn from the International Standards Organisation (ISO)[13], as follows:

- **Risk analysis**. Risk analysis is the 'systematic use of available information to identify hazards and to estimate the risk'.
- **Risk assessment.** Risk assessment is the 'overall process comprising [risk identification,] a risk analysis and a risk evaluation'. Some sources interchange 'analysis' and 'assessment'.
- **Risk evaluation**. Risk evaluation is the 'process based on risk analysis to determine whether the tolerable risk [will be] achieved'.

13 https://www.iso.org/standard/65694.html

- **Risk management**. Risk management is the proactive control and evaluation of risks via policies and management decisions.

The overall risk management process can be represented graphically, as shown in Figure 5 below.

In some countries, there are already regulations and/or best practice guides are already in place. For example, in the United Kingdom there are two guides published by the Construction Industry Research and Information Association (CIRIA), namely CIRIA Report C681 and CIRIA Report C785. In Germany there is the Construction guidelines for explosive ordnance clearance (BFR KMR) ('Kampfmittelräumung (BFR KMR) Baufachliche Richtlinien' in the original German). In Vietnam there is a regulation called Decree No. 18/2019/ND-CP.

In circumstances where there are no specific regulations or where existing regulations do not provide sufficient guidance, the following four-step risk management process is proposed:

1. Risk assessment
2. Non-technical survey (NTS)
3. Technical survey (TS) (including area reduction)
4. Full clearance

Note that full clearance is only recommended if all previous steps suggest it is necessary. It is, in effect, the risk management option of last resort.

There is no need to describe steps 2-4 in detail here. These are covered in detail in the various relevant IMAS or national technical standard or guideline (NTSG). The main issue is to understand how an initial risk assessment might work and how the findings might trigger subsequent mine action activities.

Risk assessment part one: risk identification

Risk identification in this context is a simple check to identify any potential historical evidence of EO contamination in the country (or region if possible). This can normally be done as a desk study.

Risk assessment part two: risk analysis

If the potential project is in a contaminated country or region, the next step in the risk assessment process is to determine how close it is to any recorded contaminated areas or any previously cleared areas. The analysis process should try to identify the presence of any indicators (direct or indirect) of the presence of EO contamination.

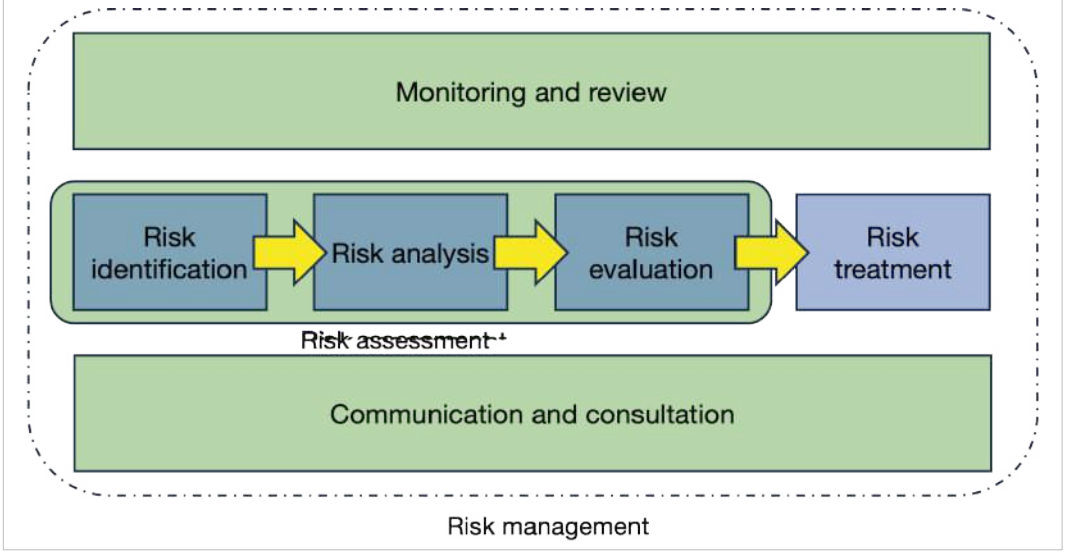


Figure 5. Graphical representation of the risk management process (ISO 13000/2018)

The presence of any indicators will suggest the need for further action. This would follow the same principles as 'land release' in humanitarian mine action, i.e. proceeding from an NTS via area reduction to clearance of any remaining contamination identified within the project area. However, in commercial projects some decisions have to be taken about the need to go further down this path. This is 'risk evaluation'.

This risk assessment procedure can be visualised as a form of a conventional 'risk matrix' as set out in **Figure 6** below. Note that it includes the unfortunately rather common situation where a site is already in use before the EO risk assessment is undertaken.

The first key point brought out by **Figure 6** is that activity affects risk. A project site not in use presents a different category of risk to one that is already in use. The second point is that any project falling into the grey category will depend on the client's appetite for risk. Likewise, the implications of a site falling into the brown category will be very context specific. Finally, it is recommended that any project that is 'red' will need immediate action, including stopping work until contamination is treated.

This risk matrix highlights the importance of the client's appetite for risk. This is discussed above but not something that is normally considered in humanitarian mine action (HMA). In HMA the evidence of absence as is implied in land release as a form of 'triage', i.e. of being sufficient in itself as a reason not to clear. This may be pragmatic in HMA where, as described above, there is a form of 'market failure' (i.e. the beneficiary of the clearance is not the customer (the donor is)) and may also be reasonable where the land is already in use for several years. However, as said by Carl Sagan, "the absence of evidence is not the same as evidence of absence", and in a commercial context the absence of evidence may be necessary but not sufficient. This leads to the recommended best practice for EO risk treatment as set out in Table 3.

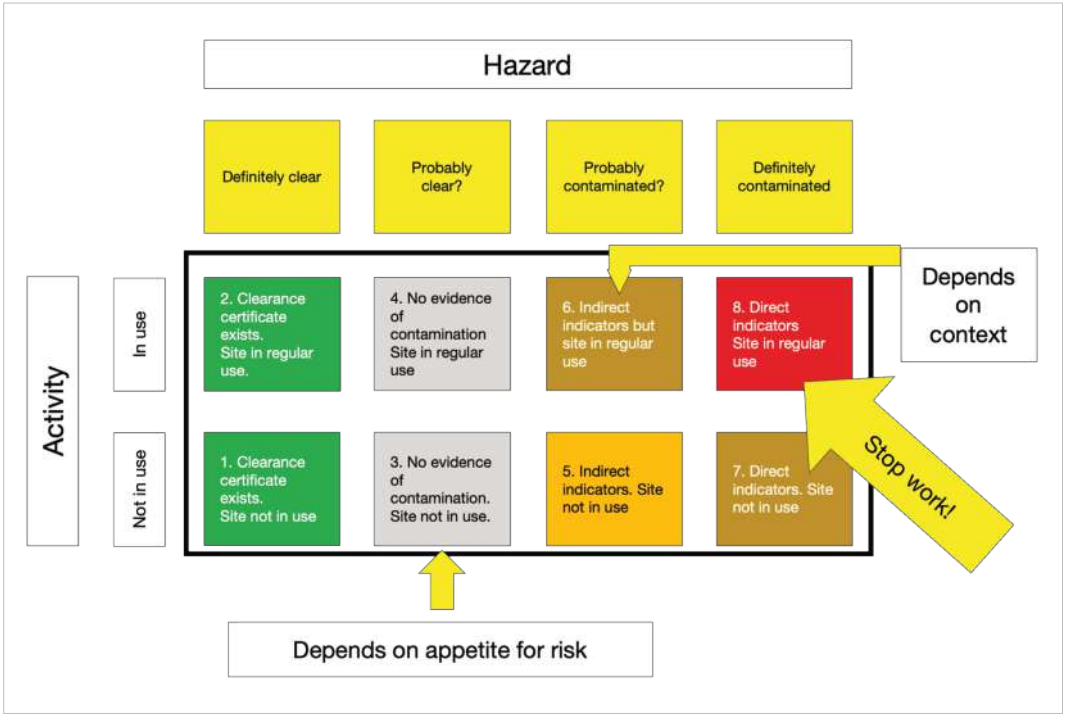


Figure 6. A form of EO risk matrix for commercial projects.

Ser	Condition	Classification	Elaboration	Recommended action	Remarks
(a)	(b)	(c)	(d)	(e)	(f)
1	Clearance certificate exists. Site in regular use.	Definitely clear	Document review can define a specific piece of ground as 'definitely clear' when (1) it has been cleared to the correct standard by a competent and accredited organisation, (2) when appropriate quality management requirements have been met, and (3) where an official clearance certificate has been issued by an appropriate authority. Furthermore, (4) the certificate must also set out the exact perimeter of the area cleared, the search method used and the depth to which a search has been undertaken.	No clearance required. Provide EORE.	Unless all four of these requirements are met, the site cannot be regarded as 'definitely' clear. Consider provision of on-call EOD response service
2	Clearance certificate exists. Site in regular use.				
3	Indirect indicators. Site not in use.	Probably clear	This may be land that does not meet the exact standards of 'definitely clear', but it may also be a piece of land where the local population has been using the land for several years without any indication that contamination is present. Another example of 'probably clear' land is land where some clearance work has been done but where the standards set out in Point #1 above cannot be met.	More information required: needs NTS. May need EORE/EOD later.	Not possible to call 'definitely clear'. Depending on appetite for risk, 'proving' the ground by use of an area reduction tool (e.g. dogs or machines) may be acceptable.
4	No evidence of contamination. Site in regular use.			Provide EORE and on-call EOD response service.	May be possible to 'disregard' clearance based on appetite for risk.
5	Indirect indicators Workforce may avoid some areas.	Probably contaminated?*	Areas identified as 'probably contaminated' are areas where there are indirect indicators of likely contamination (such as proximity to a defensive position) or where local behaviour avoids the land because of the perception of contamination.	Area reduction/TS recommended.	Need to understand workforce behaviour
6	Indirect indicators but site in regular use.			NTS and/or area reduction/TS recommended.	*This is very context specific.
7	Direct indicators. Site not in use.	Definitely contaminated	Definitely contaminated areas are areas where there are 'direct' indicators of contamination, such as visible EO presence, records of laying minefields or records of EO casualties. In order to properly define an area as 'definitely contaminated' it is usually necessary to be able to define the boundary of the contamination.	Conduct clearance in line with project works plan	Type of clearance may vary due to context. Battle Area Clearance (BAC) may be sufficient in some circumstances.
8	Direct indicators. Site in regular use.			**IMMEDIATE** clearance required	Cease works until site clear.

Table 3. Recommended risk management/treatment approach for commercial project sites

One relevant concept in risk management is that of 'Source-Pathway-Receptor' (SPR)[14]. These are defined in Box 5 below.

- **Source**. A contaminant or pollutant that is in, on or under the land and that has the potential to cause harm or pollution.
- **Pathway**. A route by which a receptor is or could be affected by a contaminant.
- **Receptor**. Something that could be adversely affected by a contaminant, for example aperson, controlled waters, an organism, an ecosystem, or Part 2A receptors such as buildings, crops or animals.

Box 5. Definitions of source, pathway and receptor as used in environmental risk management.

In the context of EO contamination it is the EO hazard that is the source of risk. The pathway is the activity conducted on a project site (either during construction or during use) and the receptor is the construction workforce, the construction equipment and the personnel who are the end-users of the project. As an example, a site in a region that has been subjected to aerial attack has different sources of hazard than one that is being built in an area that was mined, and pathways would be different in an area where foundations are required to be dug, compared to an area where people just needed to walk. This has implications for the scope of works of EO risk treatment, as discussed below. Similarly, battle area clearance using visual surface search may be sufficient, depending on context. A matrix showing how the SPR concept could be used in a project potentially contaminated with EO is included at **Annex A**.

SCOPE OF WORKS

One area where project managers can reduce the costs of clearance (and hence change the balance of project risk) is to limit (and clearly define) the scope of works for a project. This will also have the benefit of reducing both physical and reputational risks from project personnel wandering out of a cleared area and having an accident involving EO outside of the project area.

Thus, project managers should provide mine clearance contractors with a detailed large-scale map of the project task site with the boundaries clearly defined. It should also include the following where these fall outside the finished boundary of the project site:

- Stores/laydown areas
- Parking areas
- Temporary site office space
- Work room for heavy plant
- Access routes

Also, thought needs to be given to the depth of clearance. Clearance agencies have three techniques available to them, namely:

- Surface (visual) search
- Shallow instrument search
- Deep instrument search

In short, the deeper the search the longer it takes and the more it costs. Search depths for shallow instrument search are normally set by the national mine action authority (NMAA); the international norm as set out in IMAS is (at the time of writing) 13cm. Deep instrument search is usually possible with handheld equipment down to 3m but can be deeper if boreholes are drilled. It should be noted that usually only aircraft bombs penetrate this deeply: for example, it is not unknown to find a large aircraft bomb at a depth of 20m, though this is admittedly rare. Deep search is very slow and expensive and should be limited to areas where foundations are to be dug and where there is a credible EO threat. The SPR process set out above helps determine the appropriate response to potential EO hazards.

Consider again the story set out in **Box 4**. If the clearance organisation had employed the four-step

14 https://www.gov.uk/government/publications/land-contamination-risk-management-lcrm/lcrm-stage-1-risk-assessment#uxo

process set out here, and encouraged the client to provide a limited scope of works, a range of more positive scenarios could have unfolded, including:

"We've done an NTS of your site and there is no evidence of contamination. You could consider the following actions to deal with residual risk…"

"We've looked at your site and have identified that only a small portion is contaminated. If you can work without that area we can mark and fence it off so that your project staff don't wander into it."

"We've looked at your site and have identified that only a small portion is contaminated. It will cost $X to clear that area"

Quite frankly, if the clearance organisation had said any of these things there is a very good chance that they would have got the work. As it was, they got nothing. Thus, a proper risk management approach is a 'win-win' for both the client and the clearance organisation.

Conversely, work to clear the oilfields in Kuwait in 1991 was an example of how a defined scope of works facilitated what was otherwise a very difficult project. The firefighters worked out that they needed an access lane of 30 metres for each well fire, and a defined working area around each fire. Clearance work was done mainly to identify cluster munition strikes and the primary search technique was a surface visual search. See **Figure 7** below.

The task planning for the Kuwait employed the 'minimum operating strip' concept as used by military airfield damage repair. In other words, what is the minimum work needed to be done in order to get the job done? Thus, even if a 30m access lane passed through a cluster munition strike, no action would be taken against any EO outside of the 30m boundary.

Figure 7. Dealing with oil fires in Kuwait, 1991. All access and working areas were searched for EO before the firefighters could gain access.

This is a profound conceptual difference to much work undertaken in HMA, which will often tend to follow lines of contamination once these have been identified.

The management of residual risk is discussed below.

It is now possible to complete the left-hand side of the risk management bow tie. This is done by adding the potential 'contributing factors'. This is shown in **Figure 8** below. Three main contributing factors have been identified. These are:

- The area has not been cleared
- EO has been found on the site
- Personnel are unaware of the hazard and/or unaware of safe behaviour

Probability of the incidence

Remembering the formal definition of risk as a function of the probability of the incidence and the severity of the outcome, it is now possible to plot various mine action 'products' as means of reducing the probability of the incidence. These can then be broken down in turn to either (a) removing the hazard or (b) changing behaviour.

There are three mine action products that are relevant in commercial work. These are:

- Area clearance
- Explosive ordnance disposal (EOD)
- Explosive ordnance risk education (EORE)

These are all defined in IMAS 04.10. However, it is worth noting that all of these focus on reducing the probability of the incidence. EORE does this by modifying behaviour, whilst EOD and area clearance

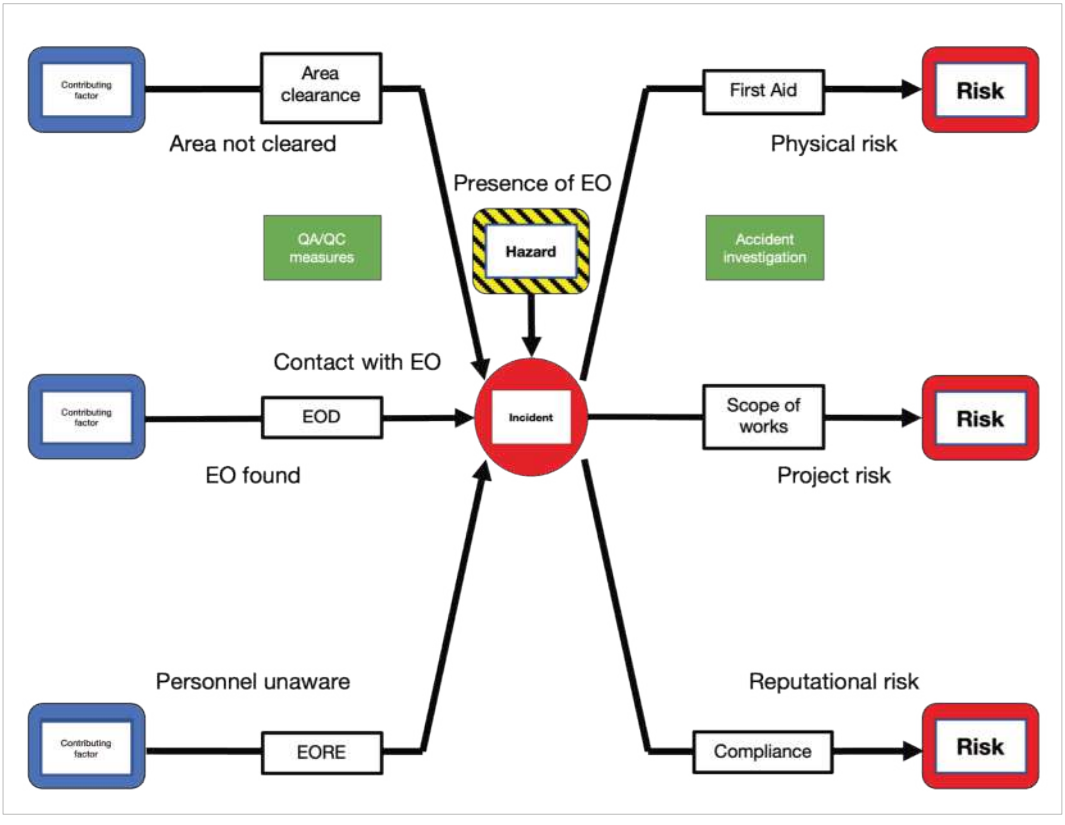


Figure 8. Building the EO risk bowtie. Note the use of quality management measures in the green boxes.

address the presence of a hazard. Area clearance does this prophylactically (an area can be searched even if definite indicators are not present) whilst EOD teams are usually deployed on a reactive basis (after the report of a possible item of EO).

In risk bowties, risk treatment options are drawn as boxes on the various causal arrows. Thus, boxes for the three mine action products have been added to **Figure 8.**

Quality management

Quality management, consisting of quality assurance (QA) and quality control (QC) play an important role in EO risk treatment, in order for the client to be sure that the risk treatment employed is fit for purpose. In the event of an incident, accident investigation is also important as it can identify any root cause (such as an inadequate scope of works) or contributing factors and thus help prevent any future incidents. These quality management measures are shown in the green boxes in **Figure 8**.

Managing the severity of the outcome

So far this paper has discussed management of the risk probability. However, it is also necessary to treat the severity of the outcome. Three boxes have been added to the right-hand side of **Figure 8**.

The severity of the outcome of physical risk can be managed to some extent by the timely availability of an adequate first aid capacity able to deal with typical EO injuries. First aid provision is discussed in IMAS 10.40. This will also, for remote sites, require a casualty evacuation plan to a hospital capable of treating typical wounds from EO.

Likewise, treatment of project risk can be done through the application of the 'scope of work' principles as set out above. This may necessitate a robust accident investigation procedure to identify any systemic issues with the mine action activities undertaken on the site.

Finally, the severity of reputational risk can be ameliorated when a project can show that it has applied 'all reasonable effort' (as discussed in IMAS Technical Note for Mine Action (TNMA) 07.11/03). If a project has established a clear scope of works, and employed relevant risk treatment through area clearance, EOD, and EORE to relevant IMAS and national standards, and where adequate first aid cover is available, then it is held that it can claim to have met the conditions of 'all reasonable effort'.

MANAGING RESIDUAL RISK

There remains the question of residual risk. This can be thought of in several ways. If the primary treatment of risk is by the prophylactic removal of hazard (within set boundaries to the appropriate standard) then the provision of EORE and an on-call EOD response to recognise and deal with items that still turn up can be considered as one way of managing residual risk. Especially under circumstances where the initial risk assessment suggested that full clearance may not have been necessary (see **Figure 6**).

However, the second way to deal with residual risk is through insurance. Insurance premiums are assessed though the insurance industry's own risk management processes, but it is possible that a project that can show compliance with the best practice suggestions set out here may benefit from reduced insurance premiums.

The willingness of an insurer to cover risk for a particular project will depend greatly on a presentation by the organisation (or their insurance broker). The presentation will need to address any questions on the risks and mitigation methods used. A broker that specialises in UXO risk coverage[15] reports that potential insurers will "want best practice as a basic requirement". The broker also stated:

> *"a poorly presented risk can end up being punitively expensive and/or end up with cover that is inadequate to protect against UXO risks"*

15 Correspondence with Jonathan Starkey of Specialist Risk Group, March 2025.

Annex A. Using the SPR approach to identifying appropriate mine action intervention

The matrix at Table 4 uses the SPR approach to identify potential receptors for different EO hazards and the possible mine action response.

Note that the end user is not always the most likely possible receptor but cannot always be ruled out, especially in areas of the project site that are not directly walked on or otherwise processed during the project construction.

The conduct of the various possible responses should in each case be conducted in accordance with the relevant IMAS/NTSG.

Ser	Potential EO hazard (source)	Pathway	Likely Receptor	Possible response	Remarks
(a)	(b)	(c)	(d)	(e)	(f)
1	Mines	• Walking the land • Handling • Digging	• Construction workers • Construction equipment • End users	Mine clearance	Including victim-operated IED functioning as improvised mines
2	Aircraft bombs	• Excavation[1]	• Construction workers • Construction equipment	Deep instrument search[2]	Potential hazard from recently deployed time-fuzed weapons. A 'soak time' may be appropriate.[3]
3	Guided weapons	• Approaching • Disturbing	• Construction workers • Construction equipment	EOD	Potential sensitive fuzing mechanisms
4	Cluster munitions	• Handling • Digging • Proximity	• Construction workers • Construction equipment • End users	Battle area clearance (shallow instrument search[3])	Potential hazard from recently deployed time-fuzed weapons. A 'soak time' may be appropriate.
5	Other LSA	• Handling • Digging	• Construction workers • Construction equipment • End users	Battle area clearance (shallow instrument search[3])	Land service ammunition other than mines
6	IED[4]	• Disturbing • Proximity	• Construction workers • Construction equipment	Search/IEDD	Potential hazard from recently deployed time-fuzed weapons. A 'soak time' may be appropriate.

Notes:

1. Defined as digging >30 cm
2. Only required in areas requiring excavation or where there is a definite indicator of a buried bomb (e.g. presence of tail unit or hole of entry)
3. Visual surface search may be sufficient on hard surfaces such as concrete or tarmac where penetration is unlikely or will be obvious on visual inspection.
4. Refers mainly to command or time delayed IED. Victim operated IED designed as improvised mines should be treated as per Ser 1; projected IED as Ser 5.

Table 4. Using the SPR approach to identifying appropriate mine action intervention

Finally, EORE remains an appropriate means to manage residual risk, as does access to an EOD response. The possible pathways in col (c) can be used to inform the contents of the EORE provided. Where EOD response is used as a treatment of residual risk, it may also be appropriate as a form of quality management to assess why the EO was not found during the initial risk treatment.

Most UXO related risks can be covered by insurance held by the clearance agency and their clients will want to see the relevant policies as part of their due diligence during the contracting process. Site owners and general construction companies can also find insurance cover for personnel and equipment. Ownership of residual risk coverage of UXO finds or incidents after the site has been handed over will depend on legislation and/or NTSG. It is hard for the contractor to maintain responsibility for a site after the clearance work has been completed: who is liable if a worker leaves the cleared area or brings an item of EO onto the site out of curiosity? This may perhaps be included in the clearance agency's insurance, but it might be more appropriate (and cost effective) to mitigate onward liability by a comprehensive quality assurance and handover process. In other words, in such an arrangement the liability of the clearance agency ends at site handover. ■

ABOUT THE AUTHOR

Dr. Robert Keeley is a former British Army Bomb Disposal Officer active in humanitarian and commercial mine action and explosive ordnance disposal (EOD) since 1991. He has worked in numerous countries and for several governments and international organisations. He specializes in project design, evaluation, and quality assurance of all aspects of mine action and has helped shape the emerging humanitarian improvised explosive device (IED) sector. Dr. Keeley is a member of the Institute of Explosives Engineers, a Member of the International Association of Bomb Technicians and Investigators, and is a Fellow of the Royal Geographical Society. He holds a PhD in Applied Environmental Economics; his thesis was on "the Economics of Landmine Clearance."

Contact Information

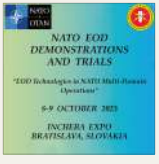
Dr. Robert Keeley, Director, RK Consulting (EOD) Ltd
Ashford, Kent, United Kingdom
Bobkeeley@rk-consulting.net
www.rk-consulting.net

UPCOMING EVENTS in 2025-26

C-IED COE Annual Conference 2025
9–12 June 2025, Malaga, Spain
https://www.ciedcoe.org/index.php/events/ciedac

12th Annual EOD/IED & Countermine Symposium
16–17 July 2025, National Harbor, MD, USA
https://countermine.dsigroup.org/

Countering Explosive Threat and Demining Conference 2025
23–24 September 2025, London, UK
https://www.defenceiq.com/events-countering-explosives/



NATO EOD Demonstrations and Trials 2025
8–9 October 2025, Bratislava, Slovakia
https://eodcoe.events/event-3/

Defense & Security 2025
10–13 November 2025, Bangkok, Thailand
https://www.asiandefense.com/

Milipol Paris 2025
18–21 November 2025, Paris, France
https://www.milipol.com/

Future Forces Exhibition & Forum 2026
21 – 23 October 2026, Prague, Czech Republic
https://www.fff.global/

Defense & Security 2025

MINISTRY OF DEFENSE
THAILAND

10–13 November 2025

IMPACT , Muang Thong Thani, **THAILAND**

Tri-Service Asian Defense & Security Exhibition,
Conference and Networking Event

Power of Partnership

info@asiandefense.com
Defense and Security 2025
Defense Security Thailand
asiandefense.com

Organised by:

GML

LANDMINE REMOVAL IN POST-CONFLICT AZERBAIJAN

By Wilder Alejandro Sánchez, President, Second Floor Strategies

The Azerbaijani government is carrying out a massive clearing operation of landmines, unexploded ordnance (UXO), and explosive remnants of war (ERW) after the 2020 and 2023 conflicts between Armenia and Azerbaijan. Baku wants to decontaminate the territories so they are fit for civilian life, however, this operation will be a lengthy, expensive, and complex process. International partners will be of vital importance for Baku to achieve this objective.

BACKGROUND

Thanks to its military victory in the Second Karabakh War (2020) and a one-day military operation on September 2023, Azerbaijan restored its territorial integrity after the loses to Armenia in the First Karabakh War (1988-1994). By 2023, negotiations resulted in the Armenian government agreeing to give up the Yerevan-controlled territorial entity known as Nagorno-Karabakh[1], now called the Karabakh Economic Region. (Due to space considerations, we will not discuss the complex historical relations, tensions, and conflict between these two countries).

Since the end of military operations, Baku and Yerevan have engaged in diplomatic negotiations for a permanent peace agreement. In mid-March[2], the two governments announced that the final text of a peace treaty had been agreed upon. However, the document has yet to be signed. (Olesya Vartanyan, a conflict analyst on the South Caucasus, has discussed the probable reasons why both governments have yet to sign the document). While discussions and negotiations continue, the removal of landmines, UXO, and other ERW is a priority as Baku has pledged that the internally displaced people due to the Karabakh wars, can return to Karabakh. Additionally, for the region to thrive, civilian infrastructure must be in place, like houses, schools, hospitals, roads, in addition to agricultural land. Landmines, UXO, and ERW must be removed to achieve this goal.

The Mine Action Review estimates that the extent of contamination is “certainly massive” as there are decades worth of tensions and military operations. Contamination is present “along the approximately 254 km-long, 5km-wide former Line of Contact (LoC) between Armenia and Azerbaijan. The defensive belts of berms, anti-tank ditches, and barbed wire along the LoC contain huge quantities of both AP and AV mines,” according to the Review. However, because of the history of inter-state tensions between Baku and Yerevan, “the areas along the LoC were heavily mined over the three decades after 1990 by all parties to the

1 https://www.britannica.com/place/Nagorno-Karabakh
2 https://eurasianet.org/a-peace-treaty-is-finalized-but-azerbaijan-is-accusing-armenia-of-preparing-for-war

conflict. Further minefields and other explosive ordnance (EO), including abandoned explosive ordnance (AXO), are found in areas previously occupied by Armenia outside Nagorno-Karabakh." In other words, the contamination of the territory goes back decades.

The Mine Action Agency of the Republic of Azerbaijan (ANAMA)[3] is the prime agency tasked with this massive operation. Other entities involved include the Ministry of Defense, the Ministry of Emergency Situations, the State Border Service, and local companies, like the Azerbaijan Demining Company and Alpha Demining[4]. Overall, 2,485 operational staff are involved in these operations, supported by 87 mine-clearing machines and 182 mine-detection dogs (Croatia has donated eight dogs), an unknown number of mine-detection rats, according to ANAMA as of late 2024. Troops are also involved in these operations, and ANAMA has conducted three-week courses for military personnel[5] on "Humanitarian Mine Clearance" and "Battlefield Cleaning." An Interagency Working Group on the Clearance of Mines and Unexploded Ordnance meets throughout the year "to review operations and enforce standards."

THE SITUATION

Decontamination operations have been ongoing since the Karabakh region fully returned to Azerbaijani control. According to ANAMA, the contamination of territory with the remnants of war reaches "60% of flat agricultural land, 30% of grassy hills, and 10% of mountainous regions." In 2023, Mine Action Review[6] estimated that 10 square kms of territory were cleared, including 3,495 anti-personnel mines destroyed (based on ANAMA info). As for 2024, a total of 62,023 hectares of Karabakh territory were decontaminated, including the removal of 59,163 pieces of unexploded ordnance, 4,286 anti-personnel mines, and 2,372 anti-tank mines. According to the most recent statistics, a total of 4,556 hectares were cleared in March 2025, which resulted in the removal of 9,755 UXO, 331 anti-personnel mines, and 105 anti-tank mines. Some of the mines neutralized include models PMN-E[7], PMN-2[8], and TM-62[9].

Anti-tank mine *(Source: ANAMA)*

As for recent operations and findings, in February, an F-1 hand grenade[10] was located near waste bins in Gazakh City, Gazakh district. Improvised explosive devices (IEDs) also contaminate the territory: an IED was located in Bulutan village, Khojavend district. The explosive consisted of one PQ-7L rocket[11], 105 small arms

3 https://anama.gov.az/en
4 https://www.alfarazminiranje.hr/?lang=en
5 https://www.azernews.az/nation/238567.html
6 https://www.mineactionreview.org/assets/downloads/Azerbaijan_Clearing_the_Mines_2024.pdf
7 https://metis.fenixinsight.com/munition/mine/pmn-e
8 https://cat-uxo.com/explosive-hazards/landmines/pmn-2-landmine
9 https://cat-uxo.com/explosive-hazards/landmines/tm-62m-landmine
10 https://anama.gov.az/en/news/302
11 https://anama.gov.az/en/news/309

IED discovered in Bulutan village, Khojavend district *(Source: ANAMA)*

cartridges attached via adhesive tape, and a hand grenade detonator, which would be triggered via tripwire.

The operation is not without incidents, and civilians who are moving to the territories remain in peril; according to ANAMA, between 2020 and 31 December 2024, there were 229 landmine explosion incidents in Karabakh, resulting in 382 victims, including 70 fatalities. The tally includes a person who stepped on a landmine in Gushchu Ayrim village, Gazakh district, last 14 October, 2024[12]. The incident occurred as the individual "while grazing animals in an area that had not been cleared of mines," which highlights the need to decontaminate areas which will be used by farmers and other field workers.

As for more recent incidents, in early April 2025, a landmine exploded in the Galaychilar village, Aghdam region. A civilian "sustained injuries[13] to his leg as a result of an anti-personnel mine explosion while entering an area that had not been cleared of landmines." Specialists tasked with removing the explosives can also be injured: in April 2025, an ANAMA employee[14] "hit an anti-personnel mine while performing his duties" in Mehdili village, Jabrayil region. He was successfully evacuated but his right leg was amputated from the ankle.

INTERNATIONAL SUPPORT

Azerbaijan will require international assistance to successfully decontaminate the Karabakh territories. Current partners include the United States, United Kingdom, European Union, Canada, Japan, and Turkiye, as well as international agencies like the United Nations Development Programme (UNDP), UNICEF, the United Nations High Commissioner for Refugees (UNHCR), the International Commission of the Red Cross (ICRC). Other actors include organizations that specialize in these types of operations, such as the Piper Demining Company[15].

Thanks to a partnership with the Geneva International Centre for Humanitarian Demining (GICHD), ANAMA "has improved its operational effectiveness through the adoption of the Information Management System for Mine Action (IMSMA)."

12 https://anama.gov.az/en/news/283
13 https://anama.gov.az/en/news/314
14 https://anama.gov.az/en/news/313
15 https://dushanbe.mfa.gov.az/ru/news/landmine-contamination-problem-in-azerbaijan

Meanwhile, the Marshall Legacy Institute[16] has contributed mine-detection dogs (MDDs); as part of a Spring 2024 visit to Azerbaijan by Institute staff, the center explained that "with 41 MLI-sponsored MDDs arriving over the last three years, ANAMA utilizes the Horadiz base to house, acclimate, and train their K9 capacity." So far the partnership between ANAMA and the Marshall Institute is working well because the dogs and the handlers are getting along, "it was rewarding to see the amazing bond formed between the MDDs and handlers," the Institute explained[17].

To increase awareness and gain international support, the Azerbaijani Ministry of Foreign Affairs and ANAMA have conducted meetings with partners and the general public. In recent months, Baku and ANAMA have met with British diplomats in Baku[18], and a meeting was held in Washington at the Hudson Institute, a think tank, to discuss this issue. Also, during the COP29 climate conference[19] held in late 2024 in Baku, ANAMA and UNDP co-organized an event titled "Clearing the Path: Addressing Mine Threats for Climate Resilience and Sustainable Development" while a photo journal exhibition titled "Silent Echoes: Untold Stories of Mine Victims"[20] was organized by Azerbaijan's embassy in Spain. Azerbaijan also participated in the 5th Review Conference of the Ottawa Convention[21], held in Siem Reap, Cambodia.

LOOKING TO THE FUTURE

The future of the removal of landmines, UXO, and ERW across Azerbaijan's territory will depend on various factors. First, a permanent peace treaty between Armenia and Azerbaijan would begin the healing process and improve relations between the two countries. Moreover, Yerevan could provide information about mine zones deployed during the conflict(s). Sharing this information would be a significant confidence-building mechanism between the two governments, and it would obviously speed up the process of decontaminating these areas.

ANAMA's explosive detection dog *(Source: ANAMA)*

As for ANAMA and other Azerbaijani agencies and organizations involved in this long-term project, unsurprisingly, budgets are a factor that limit the speed of the programs. "Since 2020, foreign assistance has accounted for merely 6% of the resources dedicated to humanitarian demining," explains the

16 https://www.marshall-legacy.org/
17 https://www.marshall-legacy.org/post/paws-of-progress-mli-donated-mdds-play-a-major-role-in-azerbaijan-s-mine-clearance-success
18 https://anama.gov.az/en/news/315
19 https://azerbaijan.un.org/en/283794-undp-and-anama-held-side-event-mine-action-and-environmental-sustainability-within-cop29
20 https://x.com/ANAMA_gov_az/status/1867605039608459587
21 https://www.apminebanconvention.org/en/review-conferences/5revcon

ANAMA's deminers *(Source: ANAMA)*

October-December 2024 Quarter Report of the agency. Countries that have donated funds include Saudi Arabia, Italy, and the United Arab Emirates. For 2025, Baku will increase ANAMA's budget to approximately USD49.9 million[22] (85 million manats), a 1.2% increase compared to last year. However, more financial assistance is necessary.

In its final 2024 Quarterly Update, ANAMA discussed several projects that require international funding and assistance. They include acquiring mine detection dogs, explosive containment chambers, explosive material transportation vehicles, ground penetrating radars (which can be mounted on a drone for faster mapping and detection operations), and demarcation and fencing markers and signs. Other requirements are directed at training and assistance, like explosive ordnance risk education, technical surveys and feasibility studies, and mine victim assistance.

There are other issues to monitor regarding how international actors can assist Azerbaijan. For example, back in 2024, UNDP and ANAMA signed a statement of intent[23] to establish an international centre of excellence and training for mine action. A year later, it is unclear if the facilities will be built but this centre would be helpful for training operations of Azerbaijani troops and other specialists. Similarly, during the Intersessional Meeting of the Anti-Personnel Mine Ban Convention last June 2024, Edson Asgarov[24], Attaché of the Permanent Representative of the Republic of Azerbaijan to the UN Office and other International Organizations in Geneva stated, "we believe that the United Nations and its specialized agencies such as UNMAS could also play a role in mobilising international support for demining operations in Azerbaijan." It is unclear if the UN Mine Action Service will start a mission in Azerbaijan, but it would be beneficial. Moreover, Mine Action Review[25] recommends that Azerbaijan

22 https://www.azernews.az/nation/235749.html
23 https://www.undp.org/azerbaijan/press-releases/undp-and-anama-signed-statement-intent-cooperation-establishment-international-centre-excellence-and-training-mine-action
24 https://www.apminebanconvention.org/fileadmin/_APMBC-DOCUMENTS/Meetings/2024/IM24-6a-Universalization-Azerbaijan.pdf
25 https://www.mineactionreview.org/assets/downloads/Azerbaijan_Clearing_the_Mines_2024.pdf

accedes to the Anti-Personnel Mine Ban Convention (APMBC)[26], adopts its revised National Mine Action Standards (NMAS), and Baku should also "finalise and adopt its new mine action strategy, reflecting the significant increase in contamination now under Azerbaijan's control."

There is one other requirement that is worth noting, and which would benefit from international support. ANAMA labels support for female demining teams as a priority. The Quarterly Report explains that "encouraging gender mainstreaming in mine action and empowering women in return, rehabilitation, reintegration and reconstruction phases." Gender diversity and the role of women as specialists who clear landmines is a topic that deserves further academic research. Without a doubt, women have also stepped forward to risk their lives for this noble cause. Afghan women[27], for example, cleared landmines before, sadly, the Taliban returned to power. Women have also stepped forward and become deminers in Zimbabwe, "When the opportunity came, I wanted to join. To show to other men, women, supporters that us women can also be deminers," said the deminer Rumbidzai[28]. Since 2017, the humanitarian organization MAG (Mines Advisory Group)[29] has been working in Zimbabwe to make land safe again for local communities – female deminers constitute around 40% of the personnel.

I have not found information about how many Azerbaijani women are involved in ANAMA's field operations. However, more female personnel would help improve gender equality, as these missions demonstrate that Azerbaijani women are just as courageous as their male counterparts. International support for mine-removal operations would, thus, have a positive collateral effect, demonstrating the bravery of Azerbaijani women.

CONCLUSIONS

If Baku and Yerevan can sign a peace treaty, permanent peace could be within reach in the South Caucasus. While peace on paper is important, so are activities on the ground. For Baku, decontaminating the Karabakh Economic Region is a priority. The data released by ANAMA and other agencies about the landmines, UXO, ERW, and IEDs located in the past couple of years demonstrate that decontamination will be a long-term project. So far, international actors have provided vital financial assistance, technical assistance, expertise, and equipment – including the invaluable mine detection dogs. However, as this analysis has demonstrated, more assistance is required for the territories to be fit for civilian life once again. ■

ABOUT THE AUTHOR

Wilder Alejandro Sánchez is an analyst who focuses on international defense, security, and geopolitical issues across the Western Hemisphere, Central Asia, and Eastern Europe. He is the President of Second Floor Strategies[30], a consulting firm in Washington, DC. He wrote an analysis on "Proliferation of Mines, Improvised Explosive Devices (IEDs) and Unexploded Ordnance (UXO) in Colombia"[31] for the Winter 2020-21 Issue of the Counter-IED Report.

26 https://www.apminebanconvention.org/en/
27 https://unfoundation.org/blog/post/innovation-in-action-brave-afghan-women-clear-landmines-make-history/
28 https://www.maginternational.org/whats-happening/the-female-lens-zimbabwe-stories/
29 https://www.maginternational.org/
30 https://secondfloor-strategies.com/
31 https://counteriedreport.com/proliferation-of-mines-improvised-explosive-devices-ieds-and-unexploded-ordnance-uxo-in-colombia/

2024-2025 THREAT DYNAMICS:
PROLIFERATION OF ONLINE INSTRUCTIONS POTENTIALLY SUPPORTING TERRORIST ATTACKS

By Lieutenant Colonel Jose M Rufas, Chief of Attack the Networks Branch, C-IED Centre of Excellence

"Never trust a man who teaches about death but yet had no real experience at all about it."
(Toba Beta in his book "Master of Stupidity", first published in 2011)

Most probably any reader would agree that the Internet has traditionally been the most effective source of technical knowledge on planning and preparation of terrorist attacks during the 21st Century.

Figure 1: Covers of publications on countering online terrorism by EUROPOL Internet Referral Unit *(Source – EUROPOL)*

Despite intensive efforts by national and multinational authorities to combat the dissemination of manuals, videos and instructions on the Internet for making improvised explosive devices (IEDs) and homemade explosives (HMEs), most (if not all) of the various publications remain available on numerous Internet sites associated with human networks linked to jihadism or other types of violent extremism (e.g. white supremacism, anarchism, eco-terrorism, far-left, separatism…).

But it is not only radical, terrorist and/or criminal organizations that are involved in distributing content on the Internet that describes:

- Planning an attack
- Acquiring precursors and components
- Manufacturing explosives, incendiary and hazardous substances
- Constructing devices…

…unfortunately, the current conflict in Ukraine is posing one of the most effective sources for terrorist performance, as based on both the widely shown ideas and the dissemination of online instructions.

The law of conservation of terrorist propaganda: online content can neither be banned nor destroyed

As previously said, most of the digital manuals on IEDs and HME manufacture are easily accessible through several online open access repositories.

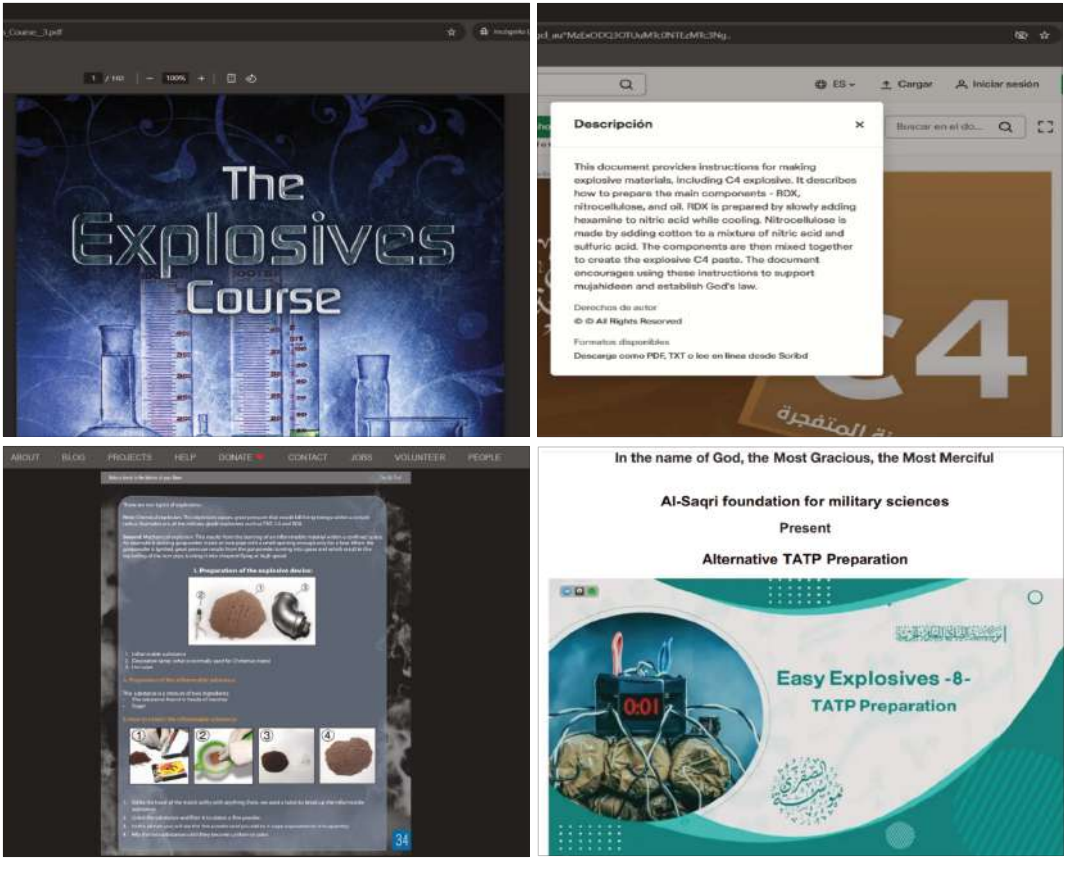


Figure 2: Jihadist HME manuals in English language found searching in browsers *(Source – WIKILEAKS, SCRIBD, ARCHIVE.ORG)*

But not only jihadism is still potentially contributing to the use of homemade explosives and improvised explosive devices: the imprudent social media supporters of both Russian and Ukrainian sides have been actively distributing videos and documents clearly showing how to manufacture homemade explosives as well as how to construct and use hundreds of different improvised explosive devices against your adversaries (or victims…). For additional information, you could read several articles published in previous issues of the 'Counter-IED Report' digital magazine...

Out of sight out of mind...

The article *'Jihadist threat dynamics concerning Europe: Are they posing a reality or just "Argumentum in Terrorem"?'* (Counter-IED Report, Winter 2024/2025 edition), predicts a significant increase in both attacks and foiled plots related to jihadism in Europe from January 2024: no doubt the next edition of Europol's European Union Terrorism Situation and Trends (TE-SAT) report will confirm this trend.

One of the first indicators identified in the first months of 2024 was a significant increase in the number of explosive-related threats on propaganda posters distributed by media outlets directly or indirectly linked to DAESH.

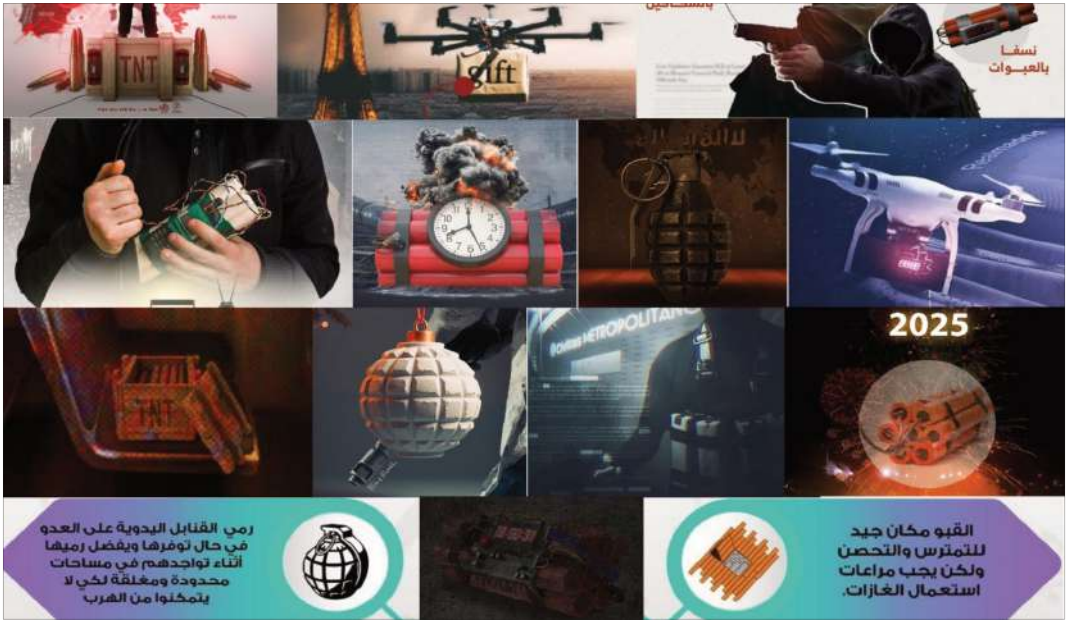


Figure 3: Composition with 2024-2025 propaganda from DAESH-related sources showing explosives *(Source – X/Telegram)*

Along with that, the interest of DAESH followers regarding HME recipes has also increased…

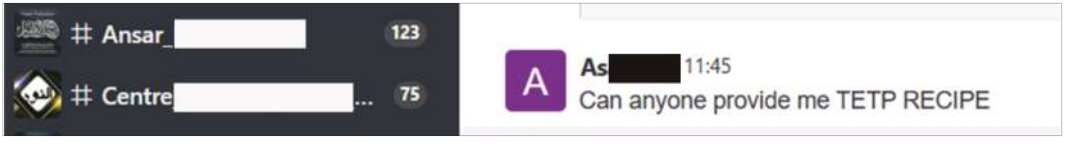


Figure 4: Capture from a DAESH-follower requesting HME information in a social media group *(Source – RocketChat)*

Information is not knowledge, but everything counts

One of the most worrying matters during 2024 and 2025 has been the diversity and location of the different sources spreading technical information about the manufacture of homemade explosives and improvised explosive devices: so along with the traditional Arabic or English language-based sources, has been identified the distribution of HME/IED instructions in Spanish, Russian, Brazilian or Turkish languages, but also in German, French, Italian… during 2024-2025.

Figure 5: Online manuals & videos in Brazilian, Turkish & Spanish languages on HME manufacture as published during 2024 *(Source – RocketChat/Youtube)*

It was quite remarkable the activity of previously known jihadist groups distributing HME/IED manuals through different social media means such as Telegram, RocketChat, Element, Chirpwire or even SImpleX: for sure, the Chechen LAMANHO group has been one of the most active during 2024, and they are still active during the first months of 2025.

The potential risk from the information as shared by LAMANHO group is mostly based on their highly didactical approach, dedication only to effective and "battle-proven" explosives, devices, and tactics plus a selection of components and precursors easy to acquire, effective to employ, and hard to track…

Figure 6: English language version of LAMANHO's catalogue of HME/IED manuals *(Source: RocketChat)*

The resurgence of the veterans

From March 2024 onwards but mostly during the first months of 2025, several accounts under the label of DAESH-related "Al Saqri Foundation for Military Sciences" have not only been redistributed but also published in different manuals in both Arabic and English languages on homemade explosives, improvised explosive devices, chemical biological radiological (CBR) agents, explosive-laden drones and terrorist/insurgent tactics, techniques and procedures.

Figure 7: Al Saqri HME & CBR related manuals as distributed/redistributed during 2025 (Source: RocketChat/Matrix)

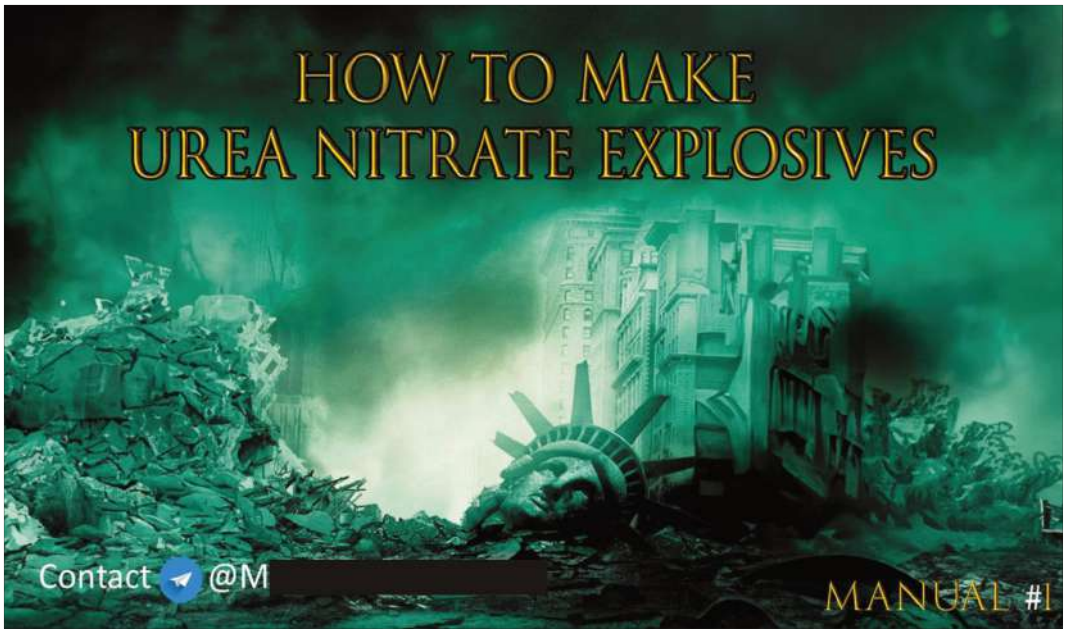
After years of ceasing to provide technical and tactical support to terrorism and insurgency, the infamous Al Saqri media office has once again taken the lead on jihadist social media.

Along with the DAESH-related initiatives, Al Qaeda followers have also published online materials in the form of videos and documents recovering technical information that was included in old issues of Al Qaeda in the Arabian Peninsula (AQAP) Al Malahem (Electronic Army) media office (e.g. INSPIRE and WOLVES OF MANHATTAN digital magazines).

Additionally, the jihadist "digital library" was also reinforced with the redistribution of hundreds of old publications on homemade explosives, improvised explosive devices, sabotage, guerrillas, improvised firearms, assassination techniques, poisons… from editors based in United States of America, possibly the Paladin Press.

Prospective

While it remains to be seen whether the trend of growing online distribution of HME/IED tutorials and videos will continue in the future, jihadist efforts to disseminate this technical and tactical information have been halted during Ramadan 2025: we shall see!



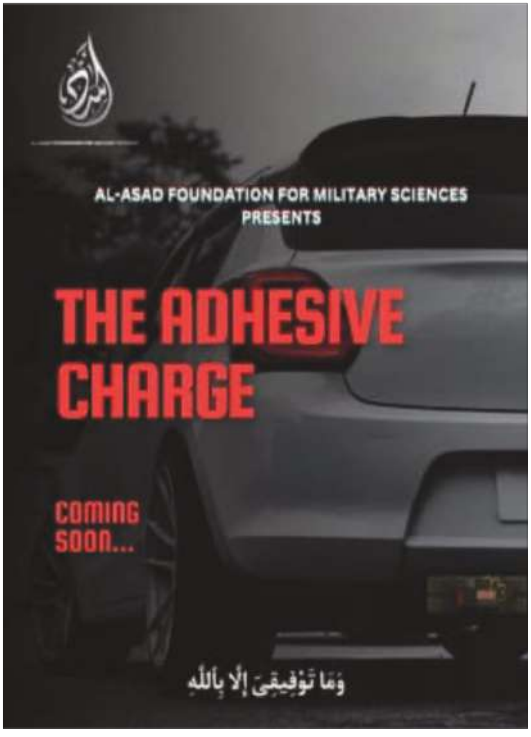


Figure 8: References to IED/HME manuals as released by alternate jihadist sources during 2024 & 2025 *(Source: X/RocketChat)*

Figure 9: References to arson and incendiary devices by jihadist propaganda during 2024 & 2025 *(Source: RocketChat/X)*

After the high impact of the recent Olympic Games and the Israeli attacks on Palestine and Lebanon, it may be difficult for jihadism to regain the rhythm of disseminating online instructions for making improvised explosive devices and homemade explosives.

Nonetheless, and in the short term, the Ukrainian conflict is for sure going to keep alive the references (and ideas) to IED manufacture and use. ■

"When working with explosives, I've found that attitude is everything."

(Alan Bradley in his book "I Am Half-Sick of Shadows", first published in 2011)

REFERENCES

- 'Jihadist threat dynamics concerning Europe: Are they posing a reality or just "Argumentum in Terrorem"?'(Counter-IED Report, Winter 2024/25 edition)
- X (former Twitter)
- Telegram
- RocketChat
- Element
- Chirpwire
- Simple X

Disclaimer

This article does not represent the opinion of any national or multinational organisation; its whole content should only be considered as the opinion of the author. As all information has been obtained from open sources, potential mistakes could have been made during the research process. Please feel free to send your comments, corrections and inputs to the author; they will be highly appreciated.

ABOUT THE AUTHOR

Lieutenant Colonel Jose M Rufas graduated from the Spanish Army Military Academy in 1993. He was commissioned into the C-IED Centre of Excellence as Head of the Defeat the Device Branch in August 2016 and currently holds the post of Chief of Attack the Networks Branch. As a Military Engineer Officer, his background has been mainly based on Explosive Ordnance Disposal activities in the Spanish Army and C-IED staff issues at the multinational headquarters. In addition to his EOD Operator / EOD Officer education, he attended some other military courses regarding Parachuting, Army Staff, Information Operations, War College General/ Joint Staff, Military Search, Technical Exploitation Operations, Weapons Intelligence Team, Exploitation Laboratories, Homemade Explosives and other C-IED courses. His operational assignments include Bosnia and Herzegovina (3), Afghanistan (3), the Republic of Ecuador, Iraq and Uganda.

E-mail: jrufas@ciedcoe.org

CALL FOR PAPERS
COUNTER-IED REPORT

Counter-IED Report editorial team invites government bodies, army personnel, researchers, industry experts to contribute their articles, case studies, white papers to the report.

We are looking for both theoretical and practice based non-promotional editorial contributions. Only original, so far not published articles are accepted.

All enquiries and articles should be submitted by email to: editorial@deltabusinessmedia.com

For more information please visit: www.counteriedreport.com/editorial

COUNTER-IED REPORT

Unique content I Global reach I In print and online

PRINT EDITION

WEBSITE

NEWSLETTER

eBOOK AND PDF

DISTRIBUTION AT THE EVENTS

Keep up-to-date with the latest C-IED, EOD and CBRNe news and developments.
Subscribe at www.counteriedreport.com/subscribe


18-21
NOVEMBER. 2025
PARIS NORD VILLEPINTE
MILIPOL
PARIS
Milipol
PARIS
Leading Event for Homeland
Security and Safety
COMEXPOSIUM
www.milipol.com
#MilipolParis
RCS Nanterre 401 138 029 - Crédits photos : Anne

CR + DR DUAL X-RAY SYSTEMS

Scanna dual radiography systems

One operating platform

Double the capability

CR + DR combined systems enable your team to respond quickly, with an optimised solution, for Counter-EO and CBRNE missions

SCANNA

X-ray Systems designed and built for bomb techs

info@scanna-msc.com

www.scanna-msc.com