

Counter-IED Report

Autumn 2024

A CONCEPTUAL FRAMEWORK FOR C-IED ENTERPRISE DESIGN

PHASES WITHIN A C-IED ENTERPRISE

DEEP LEARNING-BASED MODERN APPROACHES FOR THE
DETECTION, CLASSIFICATION AND NEUTRALIZATION OF IEDs

ENHANCING EOD OPERATIONS WITH SHERLOCK SECURITY:
ADVANCED IMAGE ANALYSIS AND THREAT DETECTION

THE LOUDEST MESSAGE: DETONATION OF COMMUNICATION
DEVICES IN LEBANON

HOUTHIS USV WBIED ATTACKS TARGETING MERCHANT SHIPS
IN THE RED SEA, YEMEN

“SAMBA JIHAD”: SOCIAL MEDIA, EXPLOSIVES AND DAESH
FOLLOWERS IN SOUTH AMERICA





Extreme 3X Dual System



AI SMART | RUGGED | DEPENDABLE



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.

© 2024. The entire contents of this publication are protected by copyright. Full details are available from the publisher. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical photocopying, recording or otherwise, without the prior permission of the copyright owner.

CONTENTS

IFC SMART RAY VISION

5 ICOR TECHNOLOGY / MED-ENG

7 GARRETT METAL DETECTORS

9 AUNAV

10 NOVO DIGITAL RADIOGRAPHY

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

13 TELEDYNE ICM

16 SAFE PRO GROUP INC.

16 3DX-RAY LTD

17 A CONCEPTUAL FRAMEWORK FOR C-IED ENTERPRISE DESIGN
By Paul Amoroso, an explosive hazards specialist at Assessed Mitigation Options (AMO) consultancy

25 VIDISCO LTD.



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

- 25 CANADIAN TECHNOLOGY SYSTEMS - CTS**
- 26 EOD/IED & COUNTERMINE SYMPOSIUM 2024**
- 27 PHASES WITHIN A C-IED ENTERPRISE**
By Paul Amoroso, an explosive hazards specialist at Assessed Mitigation Options (AMO) consultancy
- 34 MILIPOL INDIA 2025**
- 35 DEEP LEARNING-BASED MODERN APPROACHES FOR THE
DETECTION, CLASSIFICATION AND NEUTRALIZATION OF
IMPROVISED EXPLOSIVE DEVICES**
By Murat Aydoğmuş, Lieutenant Commander (OF-3) TUR-N,
Electronic Warfare Specialist, C-IED Centre of Excellence
- 41 HOMELAND SECURITY EXPO 2025**
- 42 SOF & IRREGULAR WARFARE SYMPOSIUM 2024**
- 43 ENHANCING EOD OPERATIONS WITH SHERLOCK SECURITY:
ADVANCED IMAGE ANALYSIS AND THREAT DETECTION**
By Marc Jansen, Head of Sales & Marketing, Teledyne ICM

Uncover the Unseen™

GARRETT®

Countermine Detectors

Find IEDs, UXO, and Mines with Garrett Detectors



Trusted worldwide, Garrett AML Pulse Induction countermine detectors save lives by finding mines, UXO, and IED threats in all-terrain conditions.



Scan for more info

CONTENTS

**47 THE LOUDEST MESSAGE: DETONATION OF COMMUNICATION
DEVICES IN LEBANON**

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

**54 HOUTHİ USV WBIED ATTACKS TARGETING MERCHANT SHIPS
IN THE RED SEA, YEMEN**

By Chief Superintendent (ret.) Michael Cardash,
Terrogeance - Global

**72 SAHA EXPO 2024 –
TÜRKİYE’S LEADING INTERNATIONAL
DEFENCE & AEROSPACE EXHIBITION**

**73 “SAMBA JIHAD”: SOCIAL MEDIA, EXPLOSIVES AND DAESH
FOLLOWERS IN SOUTH AMERICA**

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

79 DEFENSE & SECURITY ASIA 2025

OBC SCANNA MSC LTD

New **aunav.NEO HD** Series 2

One size fits all.



**Whether the way is narrow or wide,
aunav.NEO HD can travel it.**

Variable geometry system | Platform self-stabilization | Plug & Play payloads | Demountable | Strength and power | Autonomous capacities





Shadow III System

Super Lightweight Portable X-Ray System!

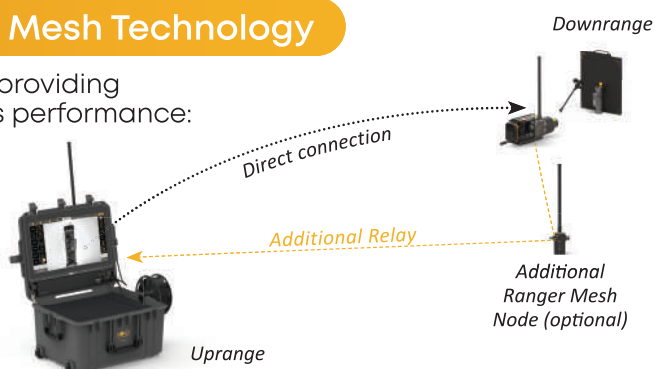
- *Android Mobile Phone operation*
- *Spark Mesh Controller - Wireless Comm*
- *Working system - only 4kg*
- *Imaging - just 3mm from bottom & side*



NOVO Wireless Mesh Technology

Unique technology providing unmatched wireless performance:

- *Strong signal stability in crowded RF environments, ideal for urban scenarios*
- *Multiple Nodes allow for working "around corners" and obstacles*



3D Arc Lite

The Lightweight Version Provides Precise Location & Exact Measurements!

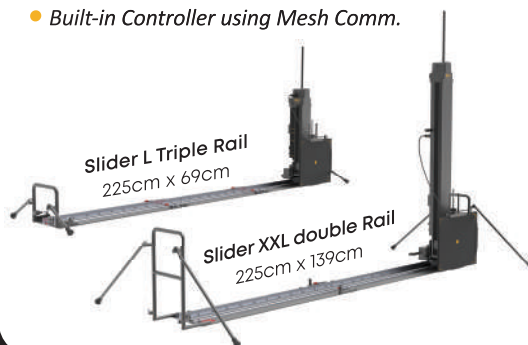
- *Provides accurate X, Y & Z coordinates of selected items*
- *Fast and easy set-up, works with any NOVO Detector*



Folding Slider L & XXL

The NOVO Folding Sliders are ideal for screening large objects

- *Built-in Controller using Mesh Comm.*



FOREWORD

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

As we move into the final quarter of 2024 two conflicts with global ramifications continue unabated – the war between Ukraine and Russia and the one in the Middle East between Israel and Iran-backed Hamas and Hezbollah. The conflict in the Middle East, in particular, has recently escalated significantly, and in the early hours of 1 October Israel crossed the border into Southern Lebanon to commence ground operations against Hezbollah military infrastructure near the border area. Improvised Explosive Devices – IEDs continue to play a pivotal role in these and other conflicts around the world.

CONFLICT IN THE MIDDLE EAST

Israel continues to demonstrate highly effective intelligence procedures enabling it to locate and neutralise senior terrorists that pose existential threats to its national security. On 31 July this year Ismail Haniyeh, the political leader of Israel's implacable enemy HAMAS, was assassinated along with his personal bodyguard in Tehran in a military run guest house used regularly by the Iranian Islamic Revolutionary Guard Corps. Haniyeh was in Tehran to attend the inauguration ceremony of the Iranian president. It is assessed that the assassination was carried out by means of an IED that had been previously emplaced, presumably by a local

employee, in the room where Haniyeh was to stay. Furthermore, it seems that the device had been in situ for a considerable length of time prior to detonation.

In late July Hezbollah military chief Fuad Shukr was killed by a targeted Israeli air strike in Beirut. Shukr was assessed to be the right-hand man of Hezbollah leader Hassan Nasrallah.¹

On 17 September large numbers of communications pagers used by Hezbollah began to detonate whilst being used in Beirut and other locations in Lebanon. Hezbollah had purchased some 5000 pagers five months earlier. Although many details are still unknown, sources close to the Lebanon security services indicated that these pagers had small amounts of explosives embedded in them. On answering a specific message purporting to emanate from the Hezbollah leadership, the pagers exploded injuring and, in some cases, killing the users. The following day similar explosions occurred in Hezbollah owned two-way radios. In total nearly forty people have been killed and some 3500 injured by the pager and two-way radio detonations. These devices were purchased by Hezbollah as they were becoming concerned by the security implications of using mobile telephones. It is assessed that these attacks were masterminded by Israel to degrade and disrupt Hezbollah command

¹ The Times of Israel dated 30 July 2024.

and communications systems.² In terms of quantities, these operations were the largest simultaneous use of IEDs to date. Lieutenant Colonel Jose Rufas of the NATO Counter-IED Centre of Excellence specifically covers these events in more detail in an article in this Edition entitled “The Loudest Message – Detonation of Communication Devices in Lebanon”. The international security and EOD communities will be closely monitoring developments as the investigation into these explosions continues. The implications for global security are significant and will require improved screening and detection technologies in personal devices used in high-risk environments.

On 20 September an Israeli airstrike on the suburbs of Beirut killed a senior Hezbollah military official, Ibrahim Aqil, commander of Hezbollah’s Radwan Guard Force. Aqil had long been sought after by the US and Israel as the mastermind of the 1983 bombing of the US Embassy in Beirut and six months later the bombings of US and French military barracks in the city. The bombings resulted in nearly 500 fatalities – US, French and Lebanese - and many life-changing injuries.³

On 27 September the top Hezbollah official, Hassan Nasrallah was killed in an Israeli airstrike on an underground compound belonging to the militant group in the Dahiyeh suburb of Beirut. It was also reported that more than 20 Hezbollah operatives were killed in this strike. Nasrallah was regarded as one of the most influential figures in the Middle East who assumed leadership of Hezbollah in 1992 and played a major role in building the group’s strength, supporting Palestinian armed group Hamas in Gaza and maintaining close ties with Iran.

UKRAINIAN CONFLICT

In early August Ukraine launched a surprise cross-border incursion into the Russian Kursk Oblast breaching Russian border fortifications and mine fields. It is estimated that about 1000sq km of the Russian territory were seized during this operation.

Both sides continue to employ land mines to deny the opposing force freedom of manoeuvre and the use of infantry. Ukraine is now one of the most landmine contaminated nations in the world. 11 of its 27 regions and more than 30% of its territory are contaminated by land mines, IEDs and various types of explosive remnants of war. In April 2024 the Ukrainian government reported that mine-related explosions have killed 296 civilians and injured 665 others since 2022. Ukraine is cooperating with more than 30 international organizations and companies and has 53 mine action operators who have received the relevant certification documents. The U.S. has pledged \$700 million in humanitarian aid to Ukraine of which \$102 million will go towards funding humanitarian demining. The U.K. has also announced a similar 600-million-pound (\$781 million) humanitarian aid package.

OTHER WORLD NEWS

The terrorist activity of Islamic State Khorasan (IS-K), a branch of the Islamic State, has been on the rise. The group has been linked to numerous attacks in 2024. The highest profile plots include a deadly attack on a concert hall in Moscow, twin bombings in Iran and foiled plans to disrupt three Taylor Swift concerts in Austria. Of all the Islamic State’s affiliates, the IS-K stands out as its most dangerous and operationally potent regional franchise, rapidly expanding transnational reach and has a robust presence in the cyber domain.

Terrorist groups in Africa continue to use IEDs to attack civilians and security personnel. Nigeria, Kenya, Mali and Somalia are among the most affected countries. According to the recent UN report at least 1,500 civilians were killed or injured by 600 improvised explosive devices (IEDs) in Somalia over the past year.

Pakistan has seen a number of terrorist attacks targeting civilians and security services in Balochistan and Khyber Pakhtunkhwa provinces.

2 BBC News of 20 September 2024.

3 UK Daily Telegraph Newspaper of 20 September 2024.

In a recent episode, a convoy of diplomats from 12 countries has been targeted by an explosion in the Swat region, causing the death of a police officer and injuring four others.

Yemen's Houthi armed group is continuing to pose threats to the maritime traffic in the region and has recently fired a 'hypersonic missile' targeting Israel.

In July, Thomas Matthew Crooks, armed with an AR-style rifle, opened fire at the former U.S. president Donald Trump while he was addressing a crowd in Butler, Pennsylvania. The shooting slightly wounded Trump, left one audience member dead and two others wounded. The suspect had a remote detonator on him. According to a federal government task force report two improvised explosive devices discovered in Thomas Crooks' car trunk were almost identical in construction. Each contained a cardboard tube filled with a grey powder that was described by a police bomb technician as having "an odor of nitromethane", the description which may suggest the presence of a fertilizer. Whether or not the suspect attempted to detonate the devices is unclear, but the report described them in a manner that cast doubt on their viability as weapons.⁴

In September, authorities in the Mexican state of Sinaloa had to deploy additional troops, shut schools and cancel a national day celebration due to out-of-control violence fuelled by infighting within the Sinaloa cartel. There are now

signs that the turf war between Sinaloa cartel factions is spreading to other northern border states of Mexico, where Los Chapitos, led by the sons of Joaquin "El Chapo" Guzman, and supporters of El Mayo Flaco, the son of arrested capo Ismael "El Mayo" Zambada, have previously shared the business of smuggling synthetic drugs into the United States.



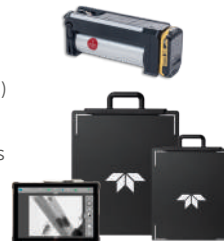
FAST & RELIABLE SOLUTION FOR EOD OPERATIONS



LiteX & TactX/XL

ULTRA-PORTABLE & COMPACT X-RAY SYSTEM

- Lightweight (2.5 Kg & 2.9/4.3 Kg)
- Battery-operated generator
- Large active area (up to 43x35 cm)
- High-quality imaging
- Reach the most inaccessible areas
- User-friendly and fast set-up
- Sherlock Security software



www.teledyneicm.com



TELEDYNE ICM
Everywhere you look™

⁴ <https://www.nytimes.com/2024/07/17/us/politics/trump-gunman-crooks-bombs.html>

IN THIS EDITION

Paul Amoroso of Assessed Mitigation Options continues his series of articles on national and regional Counter-IED efforts. In previous articles in Counter-IED Report Spring/Summer 2024 he has advocated the establishment of C-IED enterprises to oversee efforts to counter IED threats. In this article he outlines the conceptual framework for C-IED enterprise design. For such an enterprise to be successful, he advocates a strategic approach which employs effective and efficient operational processes in support of optimal tactical and technical capabilities and capacities. A strategic plan is required to demonstrate the aims and objectives of the enterprise. The article outlines the key processes for setting up the enterprise and these are a Baseline Assessment to inform the Strategic Plan, Development of the Strategic Plan and finally the Operationalisation of the Plan. He describes the ends-ways-means process in enterprise design which involves identifying and then working towards the desired end state. It may be necessary to phase the approach taken to countering IEDs depending on the operational context. He describes a possible spectrum of the use of IEDs by criminals, terrorists, insurgents through to open warfare. The response spectrum may range from Criminal Justice, CT, COIN, to a War Model and combat engineering. The author concludes that his proposed design of a C-IED enterprise, provides a platform by which it is best positioned to implement its strategic plan in a manner that it is most likely to effectively and efficiently respond to and ultimately prevent IED use.

In his second article the author examines why there is often a need for a C-IED enterprise to be able to transition between phases as it works towards the final aim of preventing IED usage. Such an enterprise is intended to counter an IED system to respond to and to ultimately prevent IED usage. The author emphasizes that the word “ultimately” is key in that it is often an aim that must be worked towards and requires different phases to match an evolving threat. The enterprise must be capable of

adapting over time. When an enterprise adopts a whole of society approach which incorporates a broad array of stakeholders it must be able to both respond to and prevent IED usage depending on the operational situation. Such an approach recognizes that preventative measures typically take longer to mature compared to purely responsive C-IED efforts. Such a challenge necessitates the need for an enterprise to transition between phases as it works towards the ultimate aim of preventing the use of IEDs. The pace and scope of such transition will be driven by the operational context within the wider security environment.

In another article Lt Col Rufas examines the exploitation and proliferation of social media platforms in South America by Islamist terrorist organisations – in particular DAESH also known as ISIS. He quotes examples of long-standing support to Islamist terrorism in South America including one example when the Islamic Jihad Organisation carried out a VBIED attack on the Israeli Embassy in Buenos Aires in March 1992. The attack killed 29 people and injured 242, destroying the Embassy and a nearby church. In January 2024 a TELEGRAM social media channel was created by two Brazilian self-proclaimed DAESH supporters. The channel became a significant repository for DAESH inspired propaganda including instructional manuals and videos on IEDs, improvised and 3D printed weapons, chemical agents and narcotics. The channel used English, Portuguese, Russian and Ukrainian languages. In August 2024 the channel started explicitly sharing information on DAESH videos with English subtitles and manuals on homemade explosives and IED manufacture. As a result of this the channel was shut down. On the 23rd anniversary of 9/11 this year a further Islamist propaganda channel was created by another Brazilian self-proclaimed DAESH supporter. The author concludes that the continuing war in the Middle East is likely to increase support for Islamist terrorism in South America.

Marc Jansen, is Head of Sales and Marketing in Teledyne ICM, which has more than 25 years of expertise in the development of innovative portable radiography solutions. In his article on Enhancing EOD Operations with Sherlock Security, he outlines the enhanced technical characteristics in the quality of X-Ray imaging which now enable the detection of previously unseen potential EOD threats. To obviate the need for an EOD operator to return to a potential explosive device, Teledyne ICM have developed filters that ensure usable images even when the initial snapshots are of suboptimal quality. In another development he describes an image stitching tool that combines multiple snapshots into a single cohesive image. Finally, he outlines the introduction of the C-View Live Video X-Ray imaging system that enables the rapid assessment of packages within seconds – operational within 90 seconds the system is ideal for time-sensitive operations.

In his article entitled “Deep Learning-Based Modern Approaches for the Detection, Classification and Neutralisation of IEDs”, Lieutenant Commander Murat Aydoğmuş of the Turkish Navy provides a highly informative overview of traditional, together with state of the art, cutting edge approaches to Counter-IED. He traces the evolution of Counter-IED technologies and procedures such as visual inspection, metal detection, sniffer systems, canine and laser detection. Building on this foundation he examines modern advances focusing on Deep Learning methodologies that have transformed IED detection and classification. Deep Learning is a subset of machine learning that uses multi-layered neural networks to simulate the brain’s decision-making power. The author examines the strengths and limitations of these approaches and offers insight into how the technologies can be integrated into a comprehensive Counter-IED framework. After examining the traditional approaches, he turns to Deep Learning techniques used for the autonomous identification and classification of IEDs. Among these he examines Convolutional Neural Networks (CNNs) that have become increasingly popular for detecting

IEDs due to their ability to learn complex patterns from visual data. He also describes other DL object detection frameworks – You Only Look Once (YOLO) Faster R-CNNs and Single Shot MultiBox Detection. Whilst describing the DL Counter-IED techniques, he highlights current limitations to these frameworks. Currently they cannot operate fully independently but require human supervision for decision making on safety grounds. Additionally, these DL systems rely on the availability of large datasets for accurate detection and classification of IEDs. The author concludes that the combination of AI and DL has significant potential to enhance IED detection and classification in the future. ■

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.

PROTECTING THOSE WHO PROTECT US ALL

NEXT-GEN DEMINING UTILIZING DRONES, AI, ML, AND BEST-OF-BREED EOD/UXO BALLISTIC PROTECTION

Serving the needs of government, military, and
humanitarian customers for over a decade



SAFE PRO GROUP
Safety with Confidence



+1-786-409-4030



INFO@SAFEPROGROUP.COM



WWW.SAFEPROGROUP.COM



ThreatScan®-AS1 (ISC)

AMORPHOUS SILICON PORTABLE X-RAY SYSTEM

Fully integrated amorphous silicon system c/w 150kV generator

High penetration with sub-millimetre resolution

Powerful image enhancement and analysis tools

For more information call

+44 (0) 1509 817400

or visit

www.3dx-ray.com

An **IMAGE SCAN** company

3DX-RAY

INSIGHT WHERE IT MATTERS



A CONCEPTUAL FRAMEWORK FOR C-IED ENTERPRISE DESIGN

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

INTRODUCTION

In previous papers¹ published in The Counter-IED Report, the author has advocated for the establishment of C-IED enterprises to counter IED systems² with the intent to respond to and ultimately prevent IED employment. A C-IED enterprise refers to the collective efforts aimed at countering IED threats.³ 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. At the heart of a C-IED enterprise are the C-IED efforts which are invested in, referring to all laws, strategies, policies, regulations, initiatives, activities, assistance, capabilities, and capacities that collectively make up a C-IED enterprise. 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.

For a C-IED enterprise to be successful, a strategic policy approach, employing effective and efficient operational processes, for its constituent elements,⁴ to support optimal tactical and technical activities, is required. This can be viewed as the alignment of the C-IED enterprise from the policy / strategic level through the operational level to the tactical / technical level. For such alignment to occur, a strategic plan, based on the assessed IED threat, is required to inform what the goal of the enterprise is. Such a strategic plan needs to include the concepts, which in this case refer to the C-IED efforts invested in, intended to achieve the goal. The C-IED efforts invested in, will inform the enterprise's structure. Finally, the resources needed to develop and

1 [*Necessity of a Designated Lead Entity within National C-IED Enterprises*](#), *The Counter-IED Report*, Spring / Summer 2024 edition, p.27. [*Nesting C-IED Appropriately within a State's National Security Architecture*](#), *The Counter-IED Report*, Spring / Summer 2024 edition, p.35.

2 The combination of people, processes, and material that go into supporting, funding, procuring, manufacturing, transporting, targeting, preparing, emplacing, executing, and publicising any element of an IED incident, including the indoctrination, training, and life support of the persons involved.

3 Countering IED threats, refers to at least matching but ideally overmatching the threat posed by the use or threatened use of IEDs.

4 C-IED elements can be considered as the parts which collectively combine to make up a C-IED enterprise. They may in some cases be individual C-IED efforts, or several C-IED efforts combined, while certain C-IED efforts may span more than one element of an enterprise.

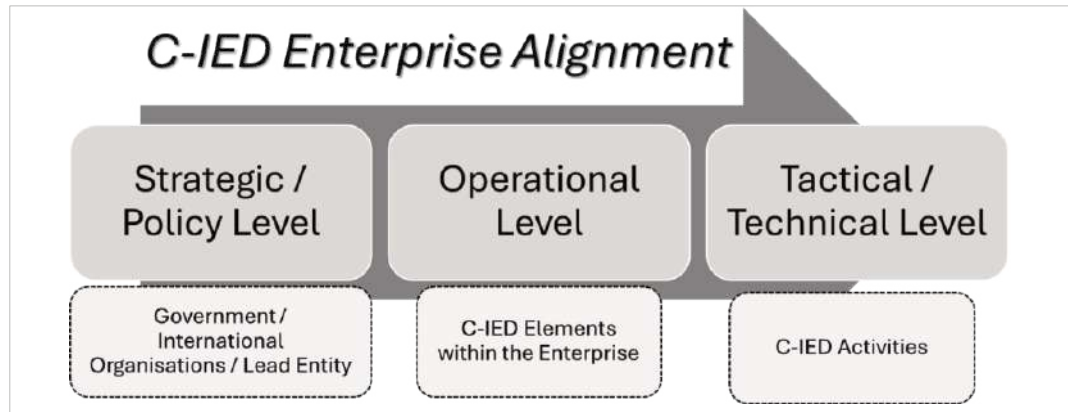


Figure 1: Concept of C-IED enterprise alignment from the strategic/policy, through the operational to the tactical/technical levels.

ultimately sustain these efforts need to be identified and secured.

Once a strategic plan is developed, it needs to be operationalised. In this case, operationalisation is taken to refer to turning a strategic plan into actionable and measurable tactical and technical C-IED activities. This involves defining specific activities, allocating resources, and establishing operational processes and subordinate tactical and technical procedures to achieve the desired goal. Operationalisation involves making an abstract strategic plan into practical and executable activities. This paper sets out a contextually adaptive, conceptual, framework for the design of a C-IED enterprise involving:

- A. Baseline assessment
- B. Strategic plan development
- C. Operationalisation

BASELINE ASSESSMENT

A baseline assessment is undertaken to determine and understand both the IED threat along with the maturity or lack thereof, of the key elements⁵ which contribute to a C-IED enterprise. Determining and understanding the IED threat being countered is often challenging and can be undertaken by a variety of methods involving many contributors and sources. It ideally involves the development and subsequent sustainment of an IED threat picture.⁶ One of the key insights that an IED threat picture can provide is an understanding of why and how IEDs are being employed as a tool of criminality, terrorism, insurgency, hybrid warfare⁷ or open warfare.⁸ This will be central in informing the subsequent strategic plan that is developed.

The UNIDIR C-IED maturity model tool can be used to assess the maturity or lack thereof, of the key elements in a C-IED enterprise. It is excellent in

5 The author has previously proposed^A 15 elements to form the basis of a C-IED enterprise based upon a synthesis of the UNIDIR C-IED SAT, the IGAD regional C-IED strategy, the AU C-IED strategy and research conducted by the author in East Africa. NOTE A: *Building the C-IED enterprise to counter the IED system*, *The Counter-IED Report*, Winter 2023 / 2024 edition.

6 An IED threat picture is an assessment of the potential use of IEDs in a defined geographical area by a stated IED system in terms of the technical complexity and tactical sophistication along with the intent of their employment, the IED system's capabilities, the opportunities for IED attacks along with local factors.

7 Hybrid warfare is a military strategy that blends conventional warfare, irregular warfare, and cyber warfare with other methods like fake news, diplomacy, and economic pressure. The goal is to create ambiguity and confusion, making it difficult for the adversary to respond effectively. A State may employ IEDs as part of the irregular warfare component of hybrid warfare, through IED attacks which are not attributable to the given adversary, or it is unclear who is responsible.

8 A situation where combat is conducted in a direct and overt manner, as opposed to covert operations or guerrilla tactics. In open warfare, both sides are clearly identifiable and engage in traditional battlefield tactics.

concept and structure, providing a methodology for analysing the reliability and sustainability of the processes, structures, and capability enabling lines of a C-IED enterprise to counter the use of IEDs. The tool uses a set of five maturity levels, with these increasing as capability improves, to support the qualitative assessment of the stakeholders' behaviours and competencies as well as the practices, processes, technology and equipment employed to reliably and sustainably respond to and ultimately prevent the use of IEDs. The tool provides a common and consistent mechanism to establish a benchmark, or a set of references, as a basis for comparison as well as a common language and frame of reference for assessing maturity and progress of C-IED capabilities. It can indicate capability gaps and areas where improvements are needed, thus providing the basis for a roadmap to identify where investment is required through national efforts or international cooperation and assistance. It can also allow the experience and lessons learned by others to be applied, thus reducing the time to introduce improvements. However, it can be challenging in terms of time, resources and expertise needed to employ it effectively. A key to its effective use is to have the most informed and empowered entity lead its employment. Such an entity needs to have the necessary influence and empowerment to have the required stakeholder community contribute to the C-IED enterprise, who will then engage with the UNIDIR tool. The information obtained from such a baseline assessment can be used to inform the development of the strategic plan for the C-IED enterprise.

STRATEGIC PLAN DEVELOPMENT

A strategic plan to countering the use of IEDs requires simultaneous and synchronized C-IED efforts at the tactical / technical, operational and strategic / policy levels. This requires a strategy that is coordinated and executed through the appropriate resourcing of the C-IED efforts chosen to be invested in. Ideally the C-IED efforts invested in should be mutually supporting and reinforcing, to effectively and efficiently respond to and ultimately prevent IED use.

There are various processes by which a strategic plan can be developed, in support of a C-IED enterprise, with the framework of ends-ways-means⁹ an effective one.¹⁰ According to Harry Yarger in his article, 'Toward a Theory of Strategy' in *Guide to National Security Policy and Strategy* published in 2006, Art Lykke gave a coherent form to a theory of strategy with his articulation of a three-legged stool model of strategy which illustrated strategy = ends + ways + means. In the Lykke model, the 'ends' are the objectives (or goal), the 'ways' are the concepts, and the 'means' are the resources for supporting the concepts. In Lykke's ends-ways-means model each part is needed to support the other for the overall strategy to be balanced. If the parts of the Lykke model are not in balance, there is an assumption of greater risk of ineffective strategy.

The requirement for balance between the three parts within a C-IED enterprise needs to be kept in mind throughout the design and subsequent sustainment of a C-IED enterprise. The desired 'ends' of a C-IED enterprise will be influenced by how IEDs are being employed, i.e. criminal, terrorist, insurgency, hybrid warfare or possibly open warfare use,¹¹ which will in turn

9 The author has previously outlined the use of an ends-ways-mean approach in the development of a seven-question framework which was applied to identify C-IED strategic principles, in *C-IED Strategic principles for East Africa*, *The Counter-IED Report*, Autumn 2023 edition.

10 The author acknowledges that Lykke's ends-ways-means strategy model provides an incomplete approach to strategic C-IED, as it fails to comprehend all its necessary dimensions. For example, there are many who deride the Lykke model for strategy, with Jeffrey W. Meiser authoring an article in *Parameter* in Winter 2016-2017 edition, entitled, 'Are Our Strategic Models Flawed? Ends + Ways + Means = (Bad) Strategy.' However, it is a framework widely used to develop strategy and can be employed and adapted to suit the context it is being applied to.

11 The author posits that countering the use of IEDs in warfare, typically involves purely military efforts, possibly only combat engineering or equivalent assets along with weapons technical intelligence activities. As such it does not typically constitute a C-IED enterprise as has been presented herein; however, a combat engineering approach may at times be necessary within a C-IED enterprise.

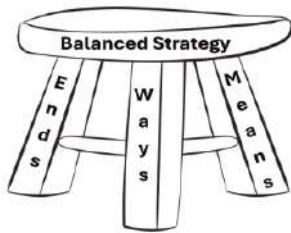


Figure 2: Three-legged stool model of balanced strategy.

influence the legal framework under which the C-IED enterprise will operate. An enterprise's legal framework will impact the 'ways' it will operate which determines the C-IED efforts that are invested in. The ideal C-IED efforts required can be identified in this logical stepwise approach; however, the actual C-IED efforts invested in will be determined by the 'means' that are available. Compromise and prioritisation are critical in this process. This gives an indication of the interdependencies of the 'ends', 'ways' and 'means' using the Lykke model for strategy and the need for balance between them.

THE ENDS OF A STRATEGIC PLAN – OVERARCHING STRATEGIC GOAL

Employing an ends-ways-means approach to a C-IED enterprise, involves firstly identifying and then working

toward a desired end-state. The desired end-state of a C-IED enterprise refers to the overarching strategic goal that the enterprise wants to achieve. The goal of a C-IED enterprise should ideally fulfil the SMART criteria¹² that are often applied when considering objectives. In doing so, a balance is required between being visionary in what the C-IED enterprise should try to achieve, while at the same time being realistic of what is most likely to be achievable. It is important to not become overly focused on assessed obstacles and inhibitors to success but to focus on what success looks like. In this sense, one may consider the overarching strategic goal to be a vision statement¹³ of what success may look like. This may be a goal that seeks to reduce the impact and effectiveness of IED employment, thus forcing an IED system to evolve and change their tactical employment of IEDs and or their technical sophistication in a manner that will be advantageous to the C-IED enterprise. Alternatively, it may be more ambitious, seeking to prevent the use of IEDs when done so in collaboration with other security, defence and development initiatives, as may be the case if a whole-of-society approach to a C-IED enterprise is adopted. Or it may be more modest in working toward containing the use of IEDs to a certain level to create the space for other stabilization,¹⁴ peacemaking¹⁵ or security development initiatives to

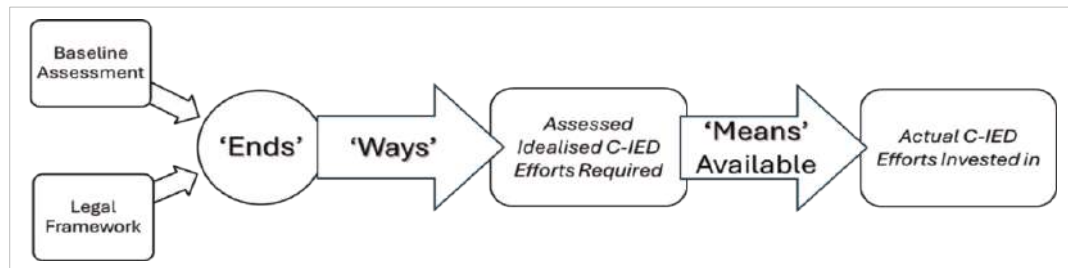


Figure 3: Interdependencies of the ends-ways-means in a C-IED enterprise.

12 Criteria that are Specific, Measurable, Achievable, Relevant and Time-Bound. SMART criteria are often used to determine whether an indicator is strong and useful for monitoring purpose. Source: *SSR in a Nutshell, Manual for Introductory Training on SSR, DCAF/ISSAT 2012*

13 In this case, a vision statement can outline what a C-IED enterprise would like to achieve, describing an idealistic and inspirational vision of its purpose, values, and goal. It can serve as a guiding principle for the enterprise's actions and decisions and should reflect its long-term aspirations.

14 A holistic approach aimed at improving security, justice, and overall stability in conflict-affected regions.

15 Deliberate actions and strategies aimed at resolving conflicts, reducing violence, and establishing conditions for lasting peace.

mature. Overall, in determining the goal it is important to appreciate that a C-IED enterprise will typically be part of wider security, defence, or development initiatives. Achieving the balance between vision and realism when developing an overarching strategic goal can be assisted by considering what good enough may be.

THE 'WAYS' OF A STRATEGIC PLAN

In considering the 'ways' of a C-IED enterprise, it is necessary to firstly assess, how IEDs are being employed, i.e. criminal, terrorist, insurgency, hybrid warfare or possibly open warfare use. For example, in a situation where IEDs are in use as a tool of criminality to intimidate, injure or kill, the goal may simply be to prevent the use or threatened use of IEDs through existing criminal justice infrastructure. In more complex conflicts involving terrorism, insurgency or open warfare, IEDs are likely to be one of multiple threats being countered. In such complex scenarios, the C-IED efforts invested in will likely form part of wider security strategies which may themselves come under broader stabilisation and even state building efforts. In such cases, C-IED efforts invested in may be part of counterterrorism, counterinsurgency or combat responses¹⁶ to wider instability or conflict. Once, how IEDs are being employed is understood, potential 'ways' or C-IED efforts for the C-IED enterprise to invest in, can be identified. Identification of potential 'C-IED efforts for an enterprise can involve deciding on:

- Required legal framework under which the C-IED enterprise will operate¹⁷ - based upon the assessed employment of IEDs;
- Constraints or limitations imposed upon the C-IED enterprise;
- Lead entity with overall responsibility for the enterprise identified and empowered;^{18,19}
- Idealised C-IED efforts, aligned to the overarching strategic goal.

When deciding the C-IED efforts to be invested in, the author has previously proposed the need for them to fit the challenging criteria of being:²⁰

- *Simple* for implementation, in often challenging operational environments, by practitioners with a wide array of training, education, skills and ability levels;
- *Agile* and responsive enough to respond to the likely evolution in the IED threat;²¹
- *Realistic* in terms of resources allocated to support its requirements;
- *Timely and responsive* in addressing and countering the use of IEDs.²²

THE 'MEANS' OF A STRATEGIC PLAN

The 'means' of a C-IED enterprise, refers to the resources needed to support the 'ways' of the strategy.²³ While each part of an ends-ways-means

16 The 2023 IGAD C-IED strategy, speaks of the war model approach to countering IED use which may be more suited for high-threat IED threat environments that are non-permissive to state security forces.

17 The author has previously written on this topic in [Legally empowered C-IED enterprises](#), *The Counter-IED Report*, Winter 2023/2024 edition.

18 The author has previously written on this topic in [Necessity of a Designated Lead Entity within National C-IED Enterprises](#), *The Counter-IED Report*, Spring/Summer 2024 edition.

19 Individual C-IED efforts, bundled under programmes and enterprises with portfolio structures may need to have sub-lead entities designated to them.

20 These challenging criteria for C-IED efforts to attain, contribute to making the management of a C-IED enterprise complex.

21 The requirement for C-IED efforts to be agile, implicitly requires the C-IED enterprise to effectively monitor their effectiveness and evaluate them to ensure they remain threat aligned. Monitoring and evaluation within a C-IED enterprise will detect such IED threat evolution.

22 Investing in and sustaining timely and responsive C-IED efforts is a challenging endeavour, being notably labour intensive; however, it is essential that benefits of the investments made are seen to deliver results in terms of effectively responding to and ultimately preventing IED incidents in an acceptable and often relatively short time frame. Such time frames can be driven by political or project management timelines.

23 The author has previously written how the 'means' involve considering the question, 'what resources we need to accomplish each effect' or alternatively, 'what resources the C-IED efforts require' in [C-IED Strategic principles for East Africa](#), *The Counter-IED Report*, Autumn 2023 edition.

approach to C-IED strategy, is equally important, the 'means' is often the part that can be most challenging to initially determine and subsequently manage. The effective and efficient management of the resources invested is the key to optimizing any C-IED enterprise. The initial resource investment needed for a given C-IED effort, should at a minimum consider the required financial, time and expertise required. However, other resources may also need to be considered in support of the required capability development. The scale that a C-IED effort will be needed at, will also need to be considered to assess the required capacity²⁴ generation. Certain tools can be employed to assist in C-IED efforts that involve capability development. For example, the US Army's C-IED strategy of 2022 advocates for the "active and continuous participation in DOTMLPF-P activities."^{25,26} Alternative frameworks include the UK's defence lines of development, TEPIDOIL model^{27,28} consisting of training, equipment, personnel, information, doctrine and concepts, organization, infrastructure, and logistics. The Finnish Defence Forces' PMDOI capability model²⁹ considers capability as a system of personnel, materiel, doctrine,³⁰ organization, and information. The author previously³¹ proposed the use of the FILLED-OIL-TIPP headings when assessing C-IED enterprise capabilities and gaps. FILLED-OIL-TIPP is an acronym for Finances/ Funding sources – Infrastructure – Logistics – Legal framework – Equipment – Doctrine & concepts – Organisation – Interoperability – Leadership – Training

– Information – Personnel – Policy. It can be used as a tool to support the assessment of capabilities and associated capacities available to respond to and ultimately prevent the use of IEDs.

From such an assessment, the 'means' required for the ideal C-IED efforts can be determined. However, ideal means are rarely available, for example, it is unlikely that the required budgets, expertise and time will be available for all the ideal C-IED efforts identified for investment. By comparing the means required for the ideal C-IED efforts to the actual means that are available, a gap analysis can be undertaken. Such gap analysis can indicate the shortfalls which may exist between required and available resources. This can then inform the decisions needed in terms of compromising between ideal C-IED efforts and the actual C-IED efforts which will be invested in. Such compromises can often involve one or more of the following options:

- Prioritization of certain C-IED efforts over others, appreciating the likely impact such changes will have on the overall C-IED enterprise;
- Provision of additional resources from elsewhere within the organization, state or region i.e. prioritization of certain C-IED efforts over other local, state or regional initiatives that need to be resourced;
- Re-examination of the ways of the C-IED enterprise, which may involve adding or removing certain constraints or limitations;

24 Capacity refers to the means of an individual/organization to perform assigned duties effectively. This includes human capacity (individual and collective competencies and experience), physical capacity (appropriate assets) and institutional capacity (systems, structures and organisational culture in place).

25 US DoD. 2022. "Army C-IED Strategy." Washington DC: US DoD, February, Page 18.

26 DOTMLPF-P pronounced "Dot-Mil-P-F," is the acronym for the US DoD model representing categories of 'solutions' such as, products and services, required to create an operational capability. It stands for the activities of Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy.

27 UK Ministry of Defence. How Defence Works. Ver. 4.2. 2015.

28 Park S-G, Lee T-G, Lim N, Son H-S. Integrated framework and methodology for capability priority decisions. Information and Security: An International Journal, Volume 25, 2010, 78-98.

29 Koivisto J, Ritala R, Vilkkio M. Conceptual model for capability planning in a military context – A systems thinking approach. Systems Engineering. 2022; 25: 457–474. <https://doi.org/10.1002/sys.21624>

30 Including tactics, techniques, and procedures (TTP).

31 The Author has previously written on the legal empowerment of C-IED enterprise in [Legally empowered C-IED enterprises: The Counter-IED Report, Winter 2023/2024 edition, p. 30-31.](#)

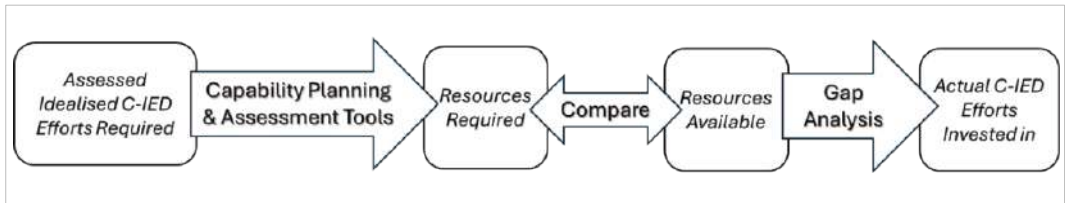


Figure 4: Identifying the C-IED Efforts to be invested in.

- In extremis, adjusting the overarching strategic goal, which will have a cascade effect on the ways and means across the C-IED enterprise;
- A combination of these options.

Such an approach to identifying the C-IED efforts to be invested in, provides a method to determine what is achievable from the available 'means', thus informing a balanced strategic plan between its 'ends', 'ways' and 'means'. In achieving such balance, a strategic plan that is manageable and optimised to the overarching strategic goal is enabled. Such an approach informs capability development and capacity generation requirements of the 'means' needed and where they are to be invested in an enterprise.

OPERATIONALISATION

The process of operationalising a C-IED strategic plan involves capturing it in a suitable document(s) and subsequently communicating it to the C-IED enterprise stakeholders. Capturing the strategic plan involves detailing the actionable and measurable C-IED activities and associated procedures, at the tactical/technical, outlining the operational processes to support the C-IED efforts invested in and how these all are aligned and coordinated to support the overarching strategic goal along with the allocated resources across all levels. Any document(s), which captures how the C-IED enterprise intends to achieve its overarching strategic goal and serves to coordinate the constituent C-IED efforts that contribute to the

enterprise in an optimised manner, can fulfil this role. It should ideally provide a roadmap to achieving the overarching strategic goal, working through the identified 'ways' and within the allocated 'means'. The document should make the abstract strategic plan into practical and executable C-IED activities.

It can be separate or a combined dedicated C-IED strategy document and associated action plan, or one or other of these. However, multiple other documents such as policy documents, doctrines, and policy statements can fulfil this requirement.³² In researching this topic, a key informant interviewee stated, "what good strategy looks like can be a challenging to define; however, those strategic documents that have proven to be effective typically communicate succinctly its why (what is intended to be done) and who must do what and by when."³³ Once the strategic plan for C-IED enterprise has been captured it needs to be communicated with the stakeholder community who make up the C-IED enterprise.

CONCLUSION

This paper presents a three component, contextually adaptable, framework intended to support the design of an appropriate C-IED enterprise to effectively and efficiently respond to and ultimately prevent IED use in line with a chosen approach involving various C-IED efforts and within available means. This framework involves a baseline assessment to ascertain the IED threat being countered as well as to assess existing current capabilities along with their capacities as well

³² *Identifying Counter Improvised Explosive Device Strategic Principles for East Africa*, Paul Amoroso, MA Strategic Studies Thesis, National University of Ireland, Cork, School of History, September 2022.

³³ Ibid.

as those capabilities needing to be developed which the C-IED enterprise will require. Following a baseline assessment, using an ends-ways-means model, a strategic plan for C-IED enterprise can be designed. Once designed it needs to be operationalized and subsequently communicated to the C-IED stakeholder community through an appropriate document(s). This design framework for a C-IED enterprise, provides a platform by which an enterprise is best positioned to implement its strategic plan in a manner that it is most likely to effectively and efficiently respond to and ultimately prevent IED use. ■

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/>

CALL FOR PAPERS

COUNTER-IED REPORT



Subscribe at:

www.counteriedreport.com/subscribe

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 theoretical and practice based non-promotional editorial contributions.*

Winter 2024/25 edition deadlines:

Abstract submission: 1 November 2024

Full article submission deadline: 5 December 2024

Publication date: 27 January 2025

Spring/Summer 2025 edition deadlines:

Abstract submission: 28 February 2025

Full article submission deadline: 15 April 2025

Publication date: 28 May 2025

Autumn 2025 edition deadlines:

Abstract submission: 18 July 2025

Full article submission deadline: 2 September 2025

Publication date: 6 October 2025

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

**Fees apply for publication of articles submitted by commercial and for-profit organisations. All articles are subject to editor's approval.*



VIDISCO
SMART PORTABLE X-RAY SOLUTIONS

DISCOVER WITH CONFIDENCE

security@vidisco.com vidisco.com

First for First Responders




PEREGRINE
The first **EOD DRONE** of it's kind
designed to be deployed with
LANCE DISRUPTER

Whether it's deployed manually, on an RoV, and now on a UAV – the Lance Disrupter has proven itself over more than 15 years, to be a leader in its field as an easy to use, effective and safe EOD tool in the bomb technician's toolbox.

- ✕ AI Object Tracking and Aiming
- ✕ 1.5cm Precision at 5m Distance
- ✕ 90° Down, 45° Up Firing Angle

CTSystems.ca • +1 514 630 0700



EOD / IED & COUNTERMINE SYMPOSIUM

CONFIRMED SPEAKERS



BRIG GEN BRIAN S. HARTLESS, USAF
DIRECTOR OF CIVIL ENGINEERS,
U.S. AIR FORCE DEPUTY CHIEF OF STAFF FOR LOGISTICS,
ENGINEERING, & FORCE PROTECTION



COL BRENNAN FITZGERALD, USA
COMMANDER, 71ST ORDNANCE GROUP



COL BRADLEY WAITE, USA
DIRECTOR, PROPONENT OFFICE FOR EOD, TRADOC



CAPT GARETH J. HEALY, USN
DEPUTY DIRECTOR FOR MILITARY PERSONNEL PLANS
& POLICY (OPNAV N13B), CHIEF OF NAVAL PERSONNEL

ACTIVE-DUTY US MILITARY/GOVERNMENT ATTEND FREE | [COUNTERMINE.DSIGROUP.ORG](https://countermine.dsigroup.org)

NOVEMBER 6-7, 2024 | NATIONAL HARBOR, MD

PHASES WITHIN A C-IED ENTERPRISE

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

INTRODUCTION

When the employment of IEDs emerges within a State or region, their use can vary depending on the context which includes, inter alia, criminal, terrorist, insurgency, hybrid warfare¹ or open warfare² use. The author has previously written³ about the development and operationalisation of a C-IED enterprise by an IED affected State. A C-IED enterprise is intended to counter an IED system through developing and sustaining the capabilities and associated capacities⁴ to respond to and ultimately prevent their employment. The C-IED enterprise that is designed, invested in and sustained will depend on the IED threat being countered and the legal framework under which it operates, which is determined by the way in which IEDs are being employed along with existing C-IED capabilities and capacities thereof. A previous paper

published in The Counter-IED Report⁵, set out 15 elements⁶ that can make up a C-IED enterprise which can be broken down into cross-cutting elements, responsive elements and preventative elements.

The author has advocated for a whole-of-society approach to C-IED as being the most comprehensive in building a C-IED enterprise, in that it encompasses the broadest number of stakeholders who can effectively respond to and prevent IED incidents. However, for several, often challenging reasons, preventing the use of IEDs is not easily achieved. This paper will examine why there is often a need for a C-IED enterprise to transition between phases as it works toward preventing their use. This is the reason why the author chooses to use the language of a C-IED enterprise working to effectively and efficiently respond

- 1 Hybrid warfare is a military strategy that blends conventional warfare, irregular warfare, and cyber warfare with other methods like fake news, diplomacy, and economic pressure. The goal is to create ambiguity and confusion, making it difficult for the adversary to respond effectively. A State may employ IEDs as part of the irregular warfare component of hybrid warfare, through the employment of IEDs which are not attributable to the given adversary, or it is unclear who is responsible.
- 2 A situation where combat is conducted in a direct and overt manner, as opposed to covert operations or guerrilla tactics. In open warfare, both sides are clearly identifiable and engage in traditional battlefield tactics.
- 3 [*A Conceptual Framework for C-IED Enterprise Design*](#), *The Counter-IED Report*, Autumn 2024 edition.
- 4 Capacity refers to the means of an individual/organization to perform assigned duties effectively. This includes human capacity (individual and collective competencies and experience), physical capacity (appropriate assets) and institutional capacity (systems, structures and organisational culture in place).
- 5 [*Building the C-IED enterprise to counter the IED system*](#), *The Counter-IED Report*, Winter 2023/2024 edition, p. 19.
- 6 Cross-cutting C-IED elements: Understanding; Preparation; Interagency and international cooperation; Information management; Adapting the C-IED enterprise. Preventative C-IED elements: National policy, regulations, and legislation; Control and security of explosives; IED precursor controls; Border controls; Intelligence led operations. Responsive C-IED elements: Defeat the device; Exploitation; Investigation; Judicial processes; Victim assistance.

to and ultimately prevent IED use. The word ‘ultimately’ is key in that it is often a goal that must be worked toward but is often challenging to achieve and requires different phases within a C-IED enterprise to match a typically evolving threat and the need for the C-IED enterprise to adapt over time.

PREVENTION IS BETTER THAN CURE

Previously it has been stated that ‘as C-IED efforts progressed in various IED affected states and regions, a recurrent lesson has been identified, which is common in most security and counter terrorism initiatives, that prevention is better than cure.’⁷ A C-IED enterprise should work to both effectively and efficiently respond to as well as ultimately prevent IED use. The preference to prevent IED use, rather than respond to their use, is self-evident in that prevention reduces the number of IED incidents and hence the need for responsive C-IED efforts to be invested in and sustained.

As C-IED develops within an IED affected State, it can initially focus on responsive C-IED efforts along with attack the network activities which target certain IED network personnel, such as those involved in the preparation, emplacement and execution activities involved in IED incidents. However, over the longer term, increased investment in preventative C-IED efforts is deemed to be more effective as responsive efforts typically have little long-term benefit as they fail to proactively and ultimately disrupt and prevent incidents. Over time, increasing investment in preventative efforts, which consider all personnel in an IED network⁸ along with the processes and materiel supply needed to support IED use, is deemed the best approach. Such targeting of all elements of an IED system can be said to be a widening of the C-IED aperture. A widened C-IED aperture will typically ‘overlap with many other defence, security, stabilization, and development initiatives such as humanitarian

mine action, weapons and ammunition management, border control, countering violent extremism, population engagement, counter / deradicalization programs, regional cooperation, counter-terrorist financing / anti-money laundering and broader counter terrorism activities.’⁹ As the C-IED aperture expands, so too does the number of stakeholders who need to be engaged which is the reason for promoting a whole-of-society approach. While acknowledging that prevention is better than cure when countering the use of IEDs, the adaptation of phases within a C-IED enterprise when pursuing a whole-of-society approach to C-IED is often necessary.

WHOLE-OF-SOCIETY APPROACHES TO C-IED – A COMPREHENSIVE APPROACH

When considering a comprehensive approach to C-IED, it is important to understand that IEDs are a weapon system and are best viewed as the symptoms of deeper underlying issues which create the conditions or ecosystem leading to their employment. To prevent the use of these weapon systems, it is crucial to first understand and address the underlying factors, problems, grievances and injustices that create the conditions for conflict, insecurity and instability leading to their employment. The root cause for the employment of IEDs can be political or ideological as well as financial or purely criminal. The theory is that if one addresses the root causes, the use of IEDs will be prevented. This typically involves the political will to provide a solution to the problems, injustices and grievances which create such conditions or alternatively achieving compromises that remedy grievances or provide redress to those who employ IEDs.

Many approaches to designing and sustaining a C-IED enterprise are possible, with a whole-of-society approach to a C-IED enterprise being advocated¹⁰ as

7 [*Building the C-IED enterprise to counter the IED system*](#), *The Counter-IED Report*, Winter 2023 /2024 edition, p. 17.

8 The IED network refers to the personnel needed to support IED incidents, including those directly involved in their supply, transport, manufacture, planning, emplacement, and execution activities, as well as those involved in indirect activities such as financing and publicising incidents, including those who facilitate such activities.

9 [*Building the C-IED enterprise to counter the IED system*](#), *The Counter-IED Report*, Winter 2023 /2024 edition, p. 17.

10 [*Building the C-IED enterprise to counter the IED system*](#), *The Counter-IED Report*, Winter 2023 /2024 edition.

being the most comprehensive and likely to prevent the employment of IEDs in the long term. It involves 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. A whole-of-society approach adopted by a C-IED enterprise aims to be comprehensive by ensuring it can both respond to IED use as well as prevent their use. Prevention is ultimately achieved by addressing the root causes that create the conditions for their use. While advocating for a whole-of-society approach to C-IED, it is acknowledged that, such approaches are not always suitable. Secondly, at times the C-IED enterprise may become overwhelmed by the IED system, forcing it to adapt in ways that may not involve a whole-of-society approach. Thirdly, a whole-of-society approach takes time to mature to the point that the use of IEDs is prevented.

OPEN WARFARE EMPLOYMENT OF IEDs

One of the contexts in which IEDs may be employed is open warfare. IEDs used in open warfare may involve the use of boobytraps¹¹ or clandestine devices¹² as well as modified items of explosive ordnance.¹³ However, it is acknowledged that countering the use of IEDs in warfare, typically involves purely military efforts, possibly employing only combat engineering or equivalent assets along with weapons technical intelligence¹⁴ activities. In open warfare, IEDs are one of multiple threats being countered, all of which will be dealt with by conventional military means. As such, it is not typically part of a C-IED enterprise as has been presented herein and the concept of phases of a C-IED enterprise would not be applicable as any efforts to counter IEDs would involve military entities only and only last as long as the war itself. However, as outlined in the section entitled 'Phases of a C-IED Enterprise,' a combat engineering approach may at times be necessary within a C-IED enterprise. The use of a 'war model approach'¹⁵ to countering IEDs is discussed later and is not necessarily related to countering the use of IEDs in open warfare.

ADAPTATION OF THE C-IED ENTERPRISE FORCED BY THE IED SYSTEM

At all times, a C-IED enterprise needs to remain effective and efficient in responding to and ultimately

- 11 Any device or material which is designed, constructed or adapted to kill or injure, and which functions unexpectedly when a person disturbs or approaches an apparently harmless object or performs an apparently safe act. Source: CCW – AP II.
- 12 A device made and conducted with secrecy by design usually for an evil or illicit purpose. Note: They do not refer to anti-handling devices or other firing mechanisms fitted to ERW, or other items of explosive ordnance being used in a manner not in their intended design role which are considered to be IEDs.
- 13 One example of this would be the modification in design or use of items of explosive ordnance as seen in the Russian full-scale invasion of Ukraine from February 2022 and in particular the use of 'bomblets' from uncrewed aerial systems.
- 14 Intelligence derived from the processes and capabilities that collect, exploit and analyse asymmetric threat weapons systems to enable material sourcing, support to prosecution, force protection, signature characterisation and targeting of threat networks. Source: UN IED Threat Mitigation Handbook, Second Edition 2024, Annex A- Lexicon.
- 15 According to the IGAD regional C-IED strategy, a war-model approach to C-IED involves a robust military led efforts, with the military having primacy in developing and implementing strategies and activities to counter the use of IEDs. This approach may be appropriate when IEDs are being used in asymmetric or hybrid warfare by an adversary. The strategy outlines the need to consider the advantages, disadvantages, and risks of using military personnel when considering adopting such a war model approach to C-IED. Source: Regional Strategy to Prevent, Counter and Respond to the Threat of Improvised Explosive Devices (IEDs) in the IGAD Region. © IGAD Security Sector Program (ISSP), www.igadssp.org
The author has previously written that a war model approach may be more suited for high-threat IED threat environments which are non-permissive to state security forces. Source: [*Legally empowered C-IED enterprises*](#), *The Counter-IED Report*, Winter 2023 /2024 edition.

preventing IED use. One of the key challenges in the initial design and development and subsequent management of a C-IED enterprise, is that the IED system will evolve to circumvent the C-IED efforts invested in against it. During the initial design and development of a C-IED enterprise, it is necessary to undertake a baseline assessment. One of the reasons for this is to develop an IED threat picture so that that C-IED efforts invested in are threat aligned. However, as an IED system evolves to circumvent the C-IED efforts invested in against it, the IED threat picture will change. A C-IED enterprise needs adaptation as one of its cross-cutting elements with the intent to adapt to IED system evolution, to remain threat aligned and ensure it is effective in responding to and ultimately preventing the employment of IEDs. However, there can be times when the evolution of the IED system overwhelms the ability of a C-IED enterprise to adapt. In such cases it may be necessary for the enterprise to move to a more response focussed approach which may also be more security or defence force centric with a reduced whole-of-society make up.

PREVENTATIVE C-IED EFFORTS TAKE TIME

When a C-IED enterprise takes a whole-of-society approach, it is important to appreciate that the preventative C-IED efforts invested in, typically take longer to mature to show effects on the IED system compared to responsive C-IED efforts. An alternative way of seeing this challenge is that compared to responsive C-IED efforts, preventative C-IED efforts take longer to see a return on investment. Preventative C-IED efforts in the long term are generally less costly and more effective than responsive efforts; however, preventative efforts are generally more resource intensive initially. As such there is the need for political understanding and backing of the benefit of investment in preventive C-IED efforts as comprehensive approaches to addressing the use of IEDs. However, a C-IED enterprise needs to be able to show impact and benefit in terms of reducing the

number of IED incidents and increasing the safety and security of the State, its citizens, and interests against the IED system. The author has previously¹⁶ discussed the challenge of needing to show such results in the development and sustainment of a C-IED enterprise. These challenges often require an initial emphasis on response focused C-IED efforts with a shift over time to preventative C-IED efforts.

CRAWL-WALK-RUN APPROACH TO PREVENTING THE USE OF IEDs

It has been outlined how preventative C-IED efforts take time to mature to show return on investment compared to responsive C-IED efforts. There is also the competing demand for a C-IED enterprise being able to show impact and benefit in terms of reducing the number of IED incidents and increasing the safety and security of the State, its citizens, and interests against the IED system. This challenge of needing to show impact against an IED system and limited initial investment in preventative efforts, can be even more pronounced in developing States with little or no existing C-IED capabilities and associated capacities. This dichotomy between wanting to invest in preventative C-IED efforts but the typical return on investment taking too long, often requires an initial response focused and even device centric investment with little or no initial investment in preventative C-IED efforts. This often sees the initial scope of a C-IED enterprise to focus on efforts which are security and defence sector centric. This may be an initial short-term phase of the C-IED enterprise.

A good starting point is to focus investment on those C-IED efforts that will have initial impact that can be pointed toward as increasing the safety and security of the State, its citizens, and interests against the IED system. One way to achieve this can be the use of quick impact projects¹⁷ when first developing a C-IED enterprise. The benefits of such quick impact projects, include, relatively speedy positive results from investments made, building confidence among the

¹⁶ *Building the C-IED enterprise to counter the IED system*, *The Counter-IED Report*, Winter 2023/2024 edition, p. 21.

¹⁷ Quick Impact Projects (QIPs) are small-scale, rapidly implementable initiatives designed to address immediate needs and build confidence in security, stabilization, and development contexts.

populace and members of the security and defence forces and encouraging further investment from funding sources. This will typically involve greater initial investment in responsive rather than preventative C-IED efforts, involving a military or security centric C-IED stakeholder community, with a C-IED enterprise that is not whole-of-society in its make-up.

When enterprises with an initial focus on responsive C-IED efforts are necessary, the imbalance between responsive and preventative efforts, can in time be addressed through the gradual but continued investment in appropriate and sustainable preventative C-IED efforts. A graduated development of a comprehensive approach to C-IED can involve a progressive expansion over several years to eventually achieve a whole-of-society C-IED enterprise with an appropriate balance of responsive and preventative C-IED efforts. Such a progression from an initial security and defence centric C-IED enterprise which is response focussed to one that is whole-of-society and has an appropriate balance of responsive and preventative C-IED efforts can be considered a crawl-walk-run approach.

A crawl-walk-run approach may involve an initial security sector centric focus which may be considered a crawling point of departure. A progressive expansion over several years to eventually achieve a comprehensive whole-of-society C-IED enterprise can be broken down under a number of phases which may involve short term, medium term, and long-term goals. Such an approach needs to be understood by all stakeholders involved to ensure coherence and in support of expectation management. How this is achieved will be determined by the management structures and practices established. When a comprehensive C-IED enterprise is achieved, space can be created that other security and stability initiatives require, not only in terms of wider state security but also within the political, economic and social domains.

PHASES OF A C-IED ENTERPRISE

In a previous Counter-IED Report paper,¹⁸ a framework for the design of a C-IED enterprise was presented

involving, a baseline assessment, the development of a strategic plan using an ends-ways-means approach, followed by its operationalisation. For the reasons outlined thus far, it may not be practical to design a C-IED enterprise which is initially focused on those C-IED efforts intended to prevent IED use.

Consequently, there may be phases to countering the use of IEDs in that one goal may be worked toward initially, with the intent in time to transition to another phase with its own defined goal. This process can in theory involve several phase transitions each of which will see the C-IED enterprise being modified to match the goal of each phase. Such phases may vary in duration involving short, medium or long-term goals being worked toward. This approach can facilitate a crawl-walk-run approach to preventing the use of IEDs. However, owing to the dynamic and evolving nature of the IED threat being countered, progress toward preventing the use of IEDs may not always be linear. Instead, phases of a C-IED enterprise may also be necessary to allow it to adapt in a manner which moves it away from a comprehensive whole-of-society approach.

When considering the phases that may be most appropriate for a given C-IED enterprise, each set of phases will vary according to the IED threat, the goal being pursued and the C-IED efforts being invested in. To appreciate the concept of the possible phases of a C-IED enterprise, examining some scenarios can be informative. One scenario could have an emerging IED threat which is addressed through a criminal justice model approach, but their use evolves over time to undermine the State and overwhelm its capacity to counter them. In such a case the C-IED enterprise may need to transition to a counterterrorism approach which is appropriately legally empowered. In situations where the threat significantly escalates, and an insurgency emerges a counterinsurgency approach may need to be adapted and in a worst-case scenario a war model approach may be needed. Such transitions between phases away from a criminal justice approach may be considered as retrograde as the intent should always be for the C-IED efforts invested in, to mature over time, with

¹⁸ *A Conceptual Framework for C-IED Enterprise Design*, The Counter-IED Report, Autumn 2024 edition.

an ultimate transition to a criminal justice approach. The stepwise retrograde transition outlined from criminal justice, to counterterrorism, to counterinsurgency and on to a war model approach may not be appropriate or possible in all scenarios. Alternatively, there is the potential to transition from a criminal justice model approach straight to a counterinsurgency or war model approach. When a State first faces an IED threat, there is also the possibility of initially adapting a counter-terrorist, counterinsurgency or war model approach, rather than a criminal justice model approach.¹⁹

In another scenario, the C-IED enterprise might initially adopt a war model approach, viewing IEDs as counter-mobility obstacles. This perspective becomes particularly relevant in cases where a State has limited or no existing C-IED capabilities and associated capacities. As such, adopting a combat engineering approach to countering them may be the initial focus. An investment in explosive ordnance disposal and weapons technical intelligence capabilities would be an example of C-IED efforts that may be prioritised in this example. Such a combat engineering phase would have an associated goal. For example, within a stated geographic area, this could involve, securing the main supply routes or ensuring freedom of manoeuvre or establishing a certain number of security bases.

An alternative scenario may involve IEDs being employed as part of a terrorist campaign within a State with existing, mature capabilities and capacities to counter them, thus allowing a counterterrorism or even a criminal justice approach. In this scenario, by adopting a counterterrorism approach to such an IED threat, the goal could be degrading the IED system to such an extent that the employment of IEDs is ineffective. This may be achieved through the prioritisation of C-IED efforts which support operations to degrade-the-system. Alternatively, in this scenario, if adopting a criminal justice approach, the goal could be prosecuting the IED system through judicial processes

intended to dismantle it in terms of its network of personnel, its materiel supply chains and its associated processes. This could be achieved through the prioritisation of all C-IED efforts needed to support the compilation of books of evidence to empower criminal prosecution.

In all cases, as transition between phases occurs, a shift in the approach taken by a C-IED enterprise will necessitate modification of existing or investment in new C-IED efforts that collectively make up the enterprise. The intent should always be for the C-IED efforts invested in, to mature over time, with an ultimate transition to a criminal justice approach. This need for transition is seen in the IGAD C-IED strategy,²⁰ which states that a war model approach to C-IED may 'prove preferable at the initial stage of countering certain IED environments but should continuously be framed in terms of and tied to goals of transition to the criminal justice model for durable C-IED capabilities and environment shaping.'

As stated in the introduction to this paper the legal framework under which a C-IED enterprise operates needs to be understood and forms the basis for how the enterprise will operate. The legal framework will most likely be determined by the way in which IEDs are being employed i.e. as a weapon system in support of criminal, terrorist, insurgency, hybrid warfare or open warfare use. In a previous C-IED Report paper,²¹ when discussing the topic of transition of a C-IED enterprise between phases, the related topic of the adaptation of the legal framework of a C-IED enterprise has been outlined. A C-IED enterprise may need to transition between phases due to an evolution in the IED threat requiring a retrograde transition away from a criminal justice approach. Alternatively, the maturing of a C-IED enterprise and related shaping of the IED system, through investment in and the effective and efficient management of appropriate C-IED efforts can allow the progressive transition toward a criminal justice

19 In all cases the approach taken should consider the threat, its scale, existing C-IED capabilities and their associated capacities, the overarching strategic goal, the C-IED efforts to be invested in and the available means for the C-IED enterprise to be developed and sustained.

20 Source: Regional Strategy to Prevent, Counter and Respond to the Threat of Improvised Explosive Devices (IEDs) in the IGAD Region. © IGAD Security Sector Program (ISSP), www.igaddssp.org

21 *Legally empowered C-IED enterprises*, *The Counter-IED Report*, Winter 2023/2024 edition.

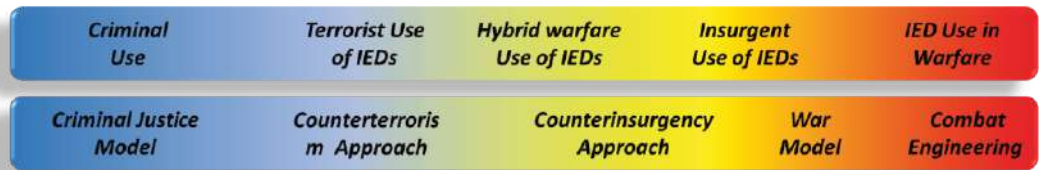


Figure 1: Spectrum of C-IED approaches.

approach. Such transition towards and away from a criminal justice approach can be visualised using a spectrum of C-IED approaches. The same concept of a spectrum of approaches to C-IED can be used to appreciate the various legal frameworks under which a C-IED enterprise can operate.

CONCLUSION

This paper advocates for a whole-of-society approach to C-IED as being comprehensive in building a C-IED enterprise, in that it encompasses the broadest number of stakeholders who can effectively respond to and prevent IED incidents. However, it has been outlined there are often challenges to preventing the use of IEDs. Most notably the dynamic and evolving nature of an IED threat along with the need for the C-IED efforts invested in to be given enough resources and time to mature to be impactful to show a return on investment. Preventative C-IED efforts typically take much longer than responsive efforts to show such return on investment. This results in the dichotomy between wanting to invest in preventative C-IED efforts but their impact against the IED system taking too long to show benefits in terms of reducing the number of IED incidents and increasing the safety and security of the State, its citizens, and interests.

These challenges necessitate the need for a C-IED enterprise to transition between phases as it works toward preventing their use. Overall, transition between various phases, moving across criminal justice, counterterrorism, counterinsurgency and combat engineering approaches, may be needed by a C-IED enterprise. Such phases may be short, medium or long term or alternatively, they may vary in duration, determined by contextual shifts owing to evolution of

the IED threat or changes in the wider security environment. This transition of a C-IED enterprise through phases may be necessary to achieve the overarching strategic goal of a comprehensive whole-of-society C-IED enterprise to effectively and efficiently respond to and ultimately prevent IED use. ■

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/>



Milipol India

The Indo- Pacific leading International Event for Homeland Security

23-25 April 2025

YASHOBHOOMI (IICC), DWARKA NEW DELHI

2ND Edition

SUPPORTED BY



INDUSTRY PARTNER



EARLY BIRD DISCOUNT

BOOK YOUR SPACE

EXHIBITOR QUERY

Harish Khanduri
(Project Manager)
8800138543
harish@interads.in

Nizam Khan
(Sr. Sales Manager)
72107 97174
nizam@interads.in

VISIT THE SHOW

VISITOR QUERY

Gayatri Chibba
(Marketing Director)
9810591686
gayatri@interads.in

- Security of Public Places
- Anti - Terrorism
- Private Security
- Data Protection
- Law Enforcement

Part of the World's
Leading Network for Homeland Security Events



ORGANIZED BY:



MEDIA PARTNER :



www.milipolindia.com

Rights to admission reserved with Inter Ads Exhibitions Pvt. Ltd., below 18 years of Age are not allowed.

DEEP LEARNING-BASED MODERN APPROACHES FOR THE DETECTION, CLASSIFICATION AND NEUTRALIZATION OF IMPROVISED EXPLOSIVE DEVICES

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

Improvised Explosive Devices (IEDs) represent a persistent and evolving threat in various conflict zones and areas of instability, demanding continuous advancements in detection and neutralization techniques in all domains. This article provides an examination of the methods used to address this challenge, tracing the evolution from traditional approaches to contemporary deep learning (DL) solutions for countermeasures against IEDs like detection and classification technologies. Initially, some conventional techniques are reviewed, including visual inspection, metal detectors and chemical sniffer systems, highlighting their operational principles. Building on this foundation, modern advancements are explored, focusing on DL methodologies that have transformed IED detection and classification. Specifically, some state-of-the-art applications like Convolutional Neural Networks (CNNs) for enhanced imaging analysis, Object Detection frameworks such as YOLO, Faster R-CNN and SSD for real-time identification are described briefly in this article. Additionally, integration of these models into unmanned systems to improve the process is investigated, and AI-driven decision support systems that assist in strategic responses are examined as

future advances. This article also addresses the challenges associated with these modern techniques, including data requirements, computational demands, and system integration issues. By examining some recent studies, case analyses, and practical applications, comprehensive understanding of the status of IED detection and classification is addressed. Additionally, future research directions aimed at improving the effectiveness and safety of these systems are provided. The findings underscore the transformative impact of DL on IED countermeasures and the ongoing need for innovation in this critical area.

INTRODUCTION

The detection, classification and neutralization of Improvised Explosive Devices (IEDs) remain critical challenges for security forces worldwide. IEDs pose a significant threat in both conflict zones and civilian environments, necessitating the development of effective countermeasures¹. Various approaches have been employed to mitigate this threat, ranging from conventional methods like visual inspection and metal detection to advanced deep learning (DL) models capable of autonomously identifying and classifying IEDs. This evolution reflects the need for a

comprehensive understanding of technologies that can both detect, classify and neutralize IEDs in diverse operational contexts².

Existing counter-IED (C-IED) strategies often lack integration between traditional and modern technological solutions, making it crucial to explore these methodologies collectively to enhance operational effectiveness³.

This survey article provides a systematic review of the state-of-the-art DL techniques in IED detection and classification, beginning with traditional techniques and progressing to advanced models. By examining the strengths and limitations of the approaches, this article aims to offer insights into how these technologies can be integrated into a comprehensive C-IED framework. The goal is to inform the community of interest and technology developers about the capabilities and gaps in current C-IED efforts.

This article aims to support the development of robust, integrated C-IED strategies that not only meet current operational needs but also anticipate future threats posed by increasingly sophisticated IED actors. Through this analysis, the paper seeks to advance the conversation on how to leverage traditional and emerging technologies to enhance global C-IED efforts.

CONVENTIONAL TECHNIQUES

Visual Inspection

Visual inspection aims to detect any signs of tampering, suspicious objects, or unusual disturbances that could indicate an IED. This method is often performed by highly trained personnel or robots. Inspecting for unusual items like wires, packages, or disturbances in soil. Looking for common IED concealment areas, such as vehicles, garbage bins, or under the ground. Signs like freshly dug ground, disturbed areas, or exposed wires might indicate the presence of an IED. It can be dangerous and time-consuming since the IED might not always be visible. Visual inspection also relies heavily on human expertise⁴.

Metal Detectors

Metal detectors are used to locate metal components in IEDs, such as the casing or wiring. While many IEDs are designed to have minimal metal to avoid detection, metal detectors are still useful in many scenarios. The detector emits electromagnetic fields, and when it passes over metallic objects, the device detects a disturbance and sends a signal. These are commonly used in tandem with ground-penetrating radar (GPR) or other sensor technologies to detect IEDs beneath the surface. IEDs made of non-metallic materials can bypass detection⁵. Also, environments with a high amount of metal debris can lead to false positives^{5,6}.

Chemical Sniffer Systems

Chemical sniffer systems are used in IED detection to identify explosive materials by detecting specific chemical signatures associated with explosives. These systems utilize various technologies, such as ion mobility spectrometry, mass spectrometry, and surface acoustic wave sensors, to analyze air samples for trace vapors emitted by explosives^{7,8,9}. They can be deployed in handheld devices or integrated into larger systems, allowing for real-time detection in various environments. Chemical sniffer systems enhance the capability to locate IEDs by identifying low concentrations of explosive substances, thereby improving overall security and threat assessment.

Ion Mobility Spectrometry (IMS) detects chemicals based on the mobility of ions in an electric field. Explosive molecules ionize and travel at different speeds depending on their size and shape. Widely used in handheld chemical sniffers and airport security scanners⁷.

Mass Spectrometry (MS) identifies chemical compounds based on the mass-to-charge ratio of ions. It's highly sensitive and can detect trace amounts of explosive materials. More commonly used in laboratory settings but can be integrated into mobile devices⁸.

Surface Acoustic Wave (SAW) These sensors detect changes in the frequency of surface acoustic waves when explosive molecules bind to a coating on the

sensor surface. Employed in portable devices for real-time detection in the field ⁹.

Laser-Based Detection

Laser-based IED detection involves using laser technology to identify explosive materials by analyzing their chemical signatures. Techniques such as Raman spectroscopy utilize laser light to detect the vibrational modes of molecules, helping to distinguish specific explosive compounds¹⁰. Quantum cascade lasers can measure how gases absorb light at wavelengths, indicating the presence of explosive vapors¹¹. These methods offer high sensitivity and specificity for detecting explosives from a distance, making them valuable tools in enhancing the safety and efficiency of IED detection operations in various environments.

Canine Detection

Although not a mechanical system, trained dogs are highly effective at detecting explosives due to their acute sense of smell. They remain widely used in conjunction with chemical sensors¹².

DEEP LEARNING BASED APPROACHES

On the other hand, with the developed technology both in terms of sensing materials and devices and their processing techniques propose a more automatized chain of operations in IED detection and neutralization. Thanks to the state-of-the-art deep learning (DL) approaches, the process has been easier in recent years.

Convolutional Neural Networks (CNNs) have become increasingly popular for detecting IEDs due to their ability to learn complex patterns from visual data. There are different kinds of imaging techniques of the data of interest. In a basic DL approach of IED detection:

- Images are captured from various sources, including surveillance cameras, drones, or ground-based vehicles etc,
- Standard CNN architectures or custom-designed models are implemented to detect/classify images if they contain IEDs or not,
- Some Techniques such as rotation, scaling, and flipping of the image are applied to increase the number of data for training and validation, thus improving model robustness.

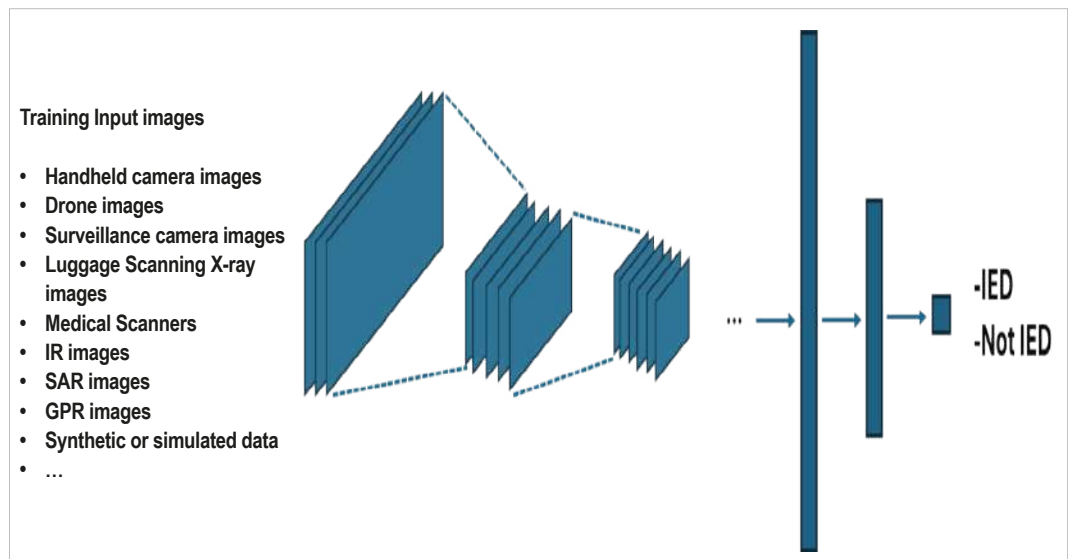


Figure 1: Simple illustration of classification as IED or not IED with a deep-learning (CNN) structure.

On the other hand, when we think of object detection frameworks like YOLO (You Only Look Once)¹³, Faster R-CNN¹⁴ and SSD (Single Shot MultiBox Detector)¹⁵, they provide many advantages and conveniences in the scope of automation. To give information very briefly about these methods:

- YOLO is a popular framework that can be used for real-time detection of different types of IEDs. YOLO can be trained to recognize different types of IEDs and their components.
- Another popular DL based IED detection method is Faster R-CNN. This method combines region proposal networks with CNNs to effectively identify and classify objects. This approach can be used to pinpoint the location of IEDs in images.
- SSD is another real-time object detection framework that can be used for IED detection in various scenarios.

These are all very common and popular tools to detect and classify IEDs and these DL based detection methods can be increased. They require a large amount of training datasets, but after a certain point, they can offer significant advantages to operators or users with their highly accurate decision-making abilities.

IEDs can take on any shape or form. Therefore, deep learning-based detection and classification require much more detail about the threat during the training phase. One of the studies shows that different shapes of IEDs, such as cylinders, squares, and spheres, can be successfully detected and classified by the deep learning algorithm based on their shapes. This means that if the database contains sufficiently rich data, it will be possible to classify IEDs and automatically alert the user using deep learning methods. This approach is applicable to systems that extract information about the target from the obtained images¹⁶.

One example on using x-ray images of luggage and containers that might contain IEDs: Images of the bags, containers are obtained with an x-ray system mounted on an autonomous vehicle and the presence of explosives is automatically reported to

the users of the system or operators. Thus, the automatic detection of IEDs based on DL and artificial intelligence systems during the execution of critical tasks offers significant advantages in terms of both cost and minimizing human casualties¹⁷.

ADVANTAGES OF THE DL BASED MODELS

DL models are excellent at extracting detailed features from sensor data, which leads to more accurate identification of IEDs. Additionally, DL based models can recognize complex patterns in the data that might be missed by traditional methods, resulting in better detection rates.

Deep learning models can be trained on varied datasets, allowing them to recognize the features of different IED types in various settings, such as urban or rural areas. These models are flexible and can adapt to different scenarios. Additionally, pre-trained models can be easily adjusted to detect new explosives or operate in different environments with minimal extra data, speeding up deployment and enhancing their capacity to handle new conditions.

After training, DL models can rapidly analyze large amounts of sensor data, enabling real-time detection of IEDs. Furthermore, DL can be incorporated into autonomous systems such as drones or robots, facilitating continuous and automated monitoring without the need for ongoing human oversight. DL models help reduce the number of false positives, which is important for avoiding unnecessary alerts or interruptions during operations.

Another important advantage of DL models is that they perform well even when dealing with noisy data. They are more robust in complex environments, such as crowded areas or rough terrains, where IEDs might be hidden.

Automating IED detection using deep learning decreases reliance on manual searches or continuous human supervision, which are often time-intensive and costly. These models can be swiftly implemented in operational environments without the need for significant extra resources, making them more economical over time.

LIMITATIONS OF DL BASED MODELS

Besides their advantages, DL systems have limitations when it comes to disarming or neutralizing IEDs. At least for now, they cannot operate independently without human supervision because the complex nature of real-time decision-making in these situations often requires human intervention for safety.

Additionally, the effectiveness of deep learning models depends on the availability of large datasets for accurate detection and classification of IEDs. However, gathering such datasets can be challenging due to the diverse range of IED designs and the various environments in which they may be encountered.

In summary, DL based IED detection systems, which offer significant advantages, especially in terms of automation, still contain some limitations and areas that need further development.

WHAT TO EXPECT IN THE FUTURE?

The future of using DL methods in detecting IEDs has promising potential for significant advancements in various areas. One direction could focus on enhancing the integration of data from multiple sensors (e.g. optical, infrared, x-ray, acoustic, chemical) using advanced DL models. Thanks to the AI techniques, this multi-modal data can be combined to provide more accurate and real-time detection, reducing false positives and improving IED identification under diverse weather and terrain conditions. Moreover, future models may become more context-aware by using DL to combine environmental factors, human activity data, and sensor input to assess the likelihood of IED presence, improving precision in complex scenarios.

By incorporating DL in multi-agent systems, where robots or drones work together with human teams, can create seamless collaboration. These systems can integrate real-time sensor data and interact dynamically to detect and neutralize IEDs in complex, hazardous environments.

One of the very important directions is to adapt to novel IED designs and emplacement strategies more quickly. Thanks to the DL based models, new types of IEDs with minimal data

could be generalized and detection and classification probabilities can be increased.

Since knowledge sharing or namely transfer learning across different domains is very important for AI systems, new research could explore how DL techniques developed for detecting IEDs in military environments can be transferred to other domains, such as border security, airport screening, or critical infrastructure protection. Cross-domain knowledge transfer can enhance the applicability of these technologies across a broader range of threat detection scenarios.

In conclusion, the future work of AI and deep learning in IED detection will likely involve more advanced, adaptive, and real-time systems that leverage multiple data sources, work autonomously and collaboratively, and integrate seamlessly with human decision-making. With continuous innovations in neural networks, robotics and sensor technologies, the potential for AI to improve IED detection and classification will expand further in the coming years. ■

REFERENCES

- 1 United Nations, "CTED Guidelines: Enhancing the Capacity of Member States to Prevent and Combat Terrorism," UN Counter-Terrorism Committee Executive Directorate, Jan. 25, 2023. [Online]. Available: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20230125_cted_guidelines_rev_en.pdf. [Accessed: Sep. 03, 2024].
- 2 United Nations Institute for Disarmament Research (UNIDIR), "Explosive Weapons in Populated Areas: A Guide for States," UNIDIR, 2023. [Online]. Available: <https://unidir.org/files/publication/pdfs/-en-641.pdf>. [Accessed: Sep. 05, 2024].
- 3 North Atlantic Treaty Organization (NATO), "Countering Improvised Explosive Devices," NATO, [Online]. Available: https://www.nato.int/cps/en/natohq/topics_77646.htm. [Accessed: Sep. 05, 2024].
- 4 United States Marine Corps, "Improvised Explosive Device (IED) Awareness," Training and Education Command, [Online]. Available: <https://www.trngcmd.marines.mil/Portals/207/Docs/TBS/B3L0487XQ-DM%20Improvised%20Explosive%20Device.pdf?ve>. [Accessed: Sep. 07, 2024].

- 5 L. E. Decker, J. H. Lentz, and R. A. Miele, "The impact of improvised explosive devices on military operations". *Naval Submarine Medical Research Laboratory*, vol. 28, no. 2, pp. 234-240, 2022. [Online]. Available: <https://onlinelibrary.wiley.com/doi/10.1002/nsg.12282>. [Accessed: Sep. 06, 2024].
- 6 Wikipedia, "Metal Detector," Wikipedia, The Free Encyclopedia, [Online]. Available: https://en.wikipedia.org/wiki/Metal_detector. [Accessed: Sep. 06, 2024].
- 7 Fetterolf, D.D. (1993). Detection of Trace Explosive Evidence by Ion Mobility Spectrometry. In: Yinon, J. (eds) Advances in Analysis and Detection of Explosives. Springer, Dordrecht. https://doi.org/10.1007/978-94-017-0639-1_13
- 8 J. Yinon, "Analysis and Detection of Explosives by Mass Spectrometry," in Aspects of Explosives Detection, M. Marshall and J. C. Oxley, Eds. Elsevier, 2009, pp. 147–169. doi: 10.1016/B978-0-12-374533-0.00008-8.
- 9 A. Mujahid and F. L. Dickert, "Surface Acoustic Wave (SAW) for Chemical Sensing Applications of Recognition Layers," Sensors, vol. 17, no. 12, p. 2716, 2017. doi: 10.3390/s17122716.
- 10 M. E. Farrell, E. L. Holthoff, and P. M. Pellegrino, 'Laser-based optical detection of explosives', 01 2015, pp. 1–8.
- 11 Block Engineering, "Active Detection of Explosives: A Technology Overview," Block Engineering, [Online]. Available: <https://www.blockeng.com/technology/active.pdf>. [Accessed: Sep. 16, 2024].
- 12 K. Frank, H. Holness, K. Furton, and L. DeGreeff, 'Explosives detection by dogs', 01 2022, pp. 47–75.
- 13 V7 Labs, "YOLO Object Detection: An Overview," V7 Labs, [Online]. Available: <https://www.v7labs.com/blog/yolo-object-detection>. [Accessed: Sep. 02, 2024].
- 14 R. Galvez and E. Dadios, 'Identifying threat objects using faster region-based convolutional neural networks (faster R-CNN)', International Journal of Advances in Intelligent Informatics, vol. 8, p. 381, 11 2022.
- 15 W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.-Y. Fu, and A. C. Berg, "SSD: Single Shot MultiBox Detector," in *Computer Vision – ECCV 2016*, Springer International Publishing, 2016, pp. 21–37. doi: 10.1007/978-3-319-46448-0_2.
- 16 S. Lameri, F. Lombardi, P. Bestagini, M. Lualdi, and S. Tubaro, "Landmine detection from GPR data using convolutional neural networks," in *25th European Signal Processing Conference, EUSIPCO 2017*, vol. 2017, 2017, pp. 508–512. doi: 10.23919/EUSIPCO.2017.8081259.
- 17 C. Chamnanphan, S. Vorapatraton, K. Kirimasthong, T. Boongoen, and N. Iam-On, 'Improvised Explosive Device Detection Using CNN With X-Ray Images', Journal of Advances in Information Technology, vol. 14, pp. 674–684, 01 2023.

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 masters' degrees in Electrical Engineering and Engineering Acoustics from the Naval Postgraduate School. His background is primarily based on Navy R&D projects. He is currently pursuing PhD studies in underwater target detection using modern deep-learning models.

Email: maydogmus@ciedcoe.org

HOMELAND SECURITY

www.eurohomeseceexpo.com EXPO

26th-27th MARCH 2025

KISTAMÄSSAN EXHIBITION & CONGRESS
CENTRE, STOCKHOLM, SWEDEN

NORDIC REGION'S ONLY AND EXCLUSIVE EXHIBITION ON

Defence, Homeland
Security, Policing,
Drone & Anti-Drone
System and many
more...



Organised By

Supported By

Media Partners



Ashish Gupta (Exhibition Director)
E-mail: ashish@nexgenexhibitions.com,
info@eurohomeseceexpo.com
Mob/Whatsapp: +91- 7533018555

For Space Booking and More Details Contact us :



SOF & IRREGULAR WARFARE SYMPOSIUM

DECEMBER 11 - 12, 2024 | TAMPA, FL



ACTIVE MILITARY & GOVERNMENT RECEIVE FREE REGISTRATION

LEARN MORE AT [SOF.DSIGROUP.ORG](https://sof.dsigroup.org)

ENHANCING EOD OPERATIONS WITH SHERLOCK SECURITY: ADVANCED IMAGE ANALYSIS AND THREAT DETECTION

By Marc Jansen, Head of Sales & Marketing, Teledyne ICM

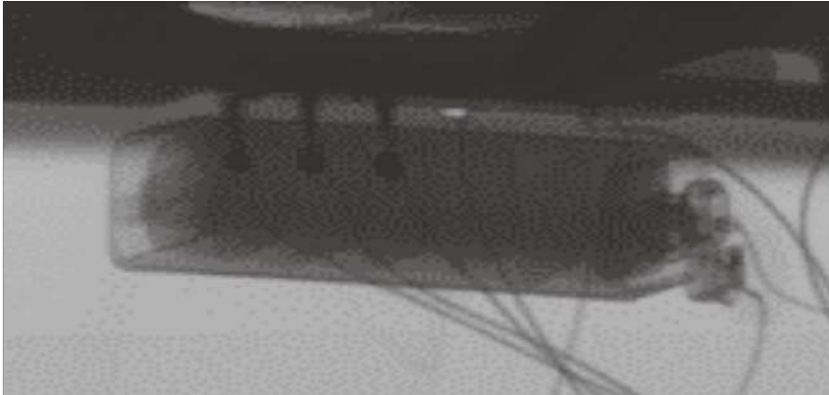
For over three decades, Teledyne ICM has been a trusted name in the manufacture of X-Ray equipment for Explosive Ordnance Disposal (EOD) teams worldwide. The evolution of technology has significantly enhanced the quality of X-Ray imaging,

enabling the detection of previously unseen threats. With advancements such as higher image definitions, precise filtering tools, and a small focal spot in the X-Ray generator, even the minutest details can now be visible.

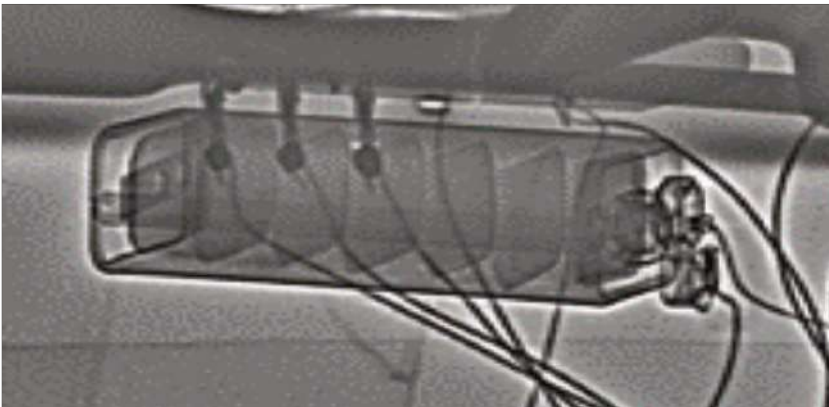


One critical concern for operators is the need to avoid returning to a potential explosive device due to poor image quality. In response to this, Teledyne ICM has developed robust filters that ensure usable images even when initial snapshots are suboptimal. Here are a few examples:

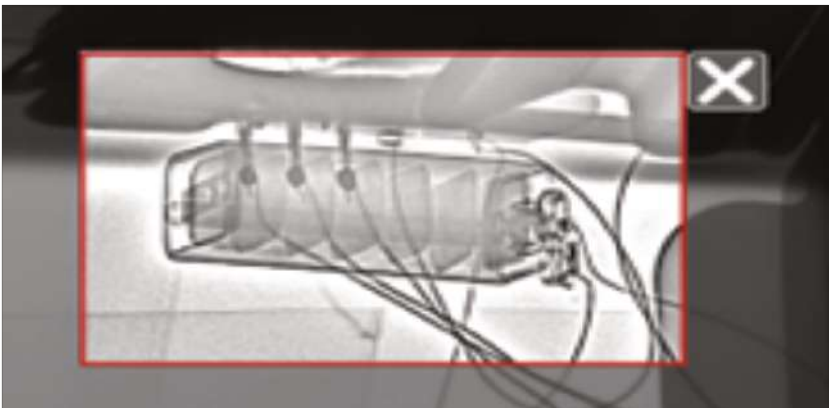
- Teledyne Filter
- Histogram adjustment
- ROI Filter
- And more.



Raw Image



Teledyne Filter



Teledyne Filter + ROI

In certain scenarios, the package requiring inspection exceeds the size of the detector, necessitating multiple images. This can complicate the inspection, identification, and decision-making

processes when dealing with separate images. To facilitate the reading, Teledyne ICM designed a stitching tool that combines multiple snapshots into a single cohesive image.

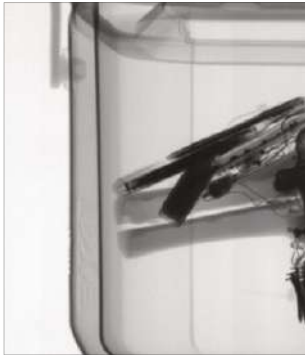


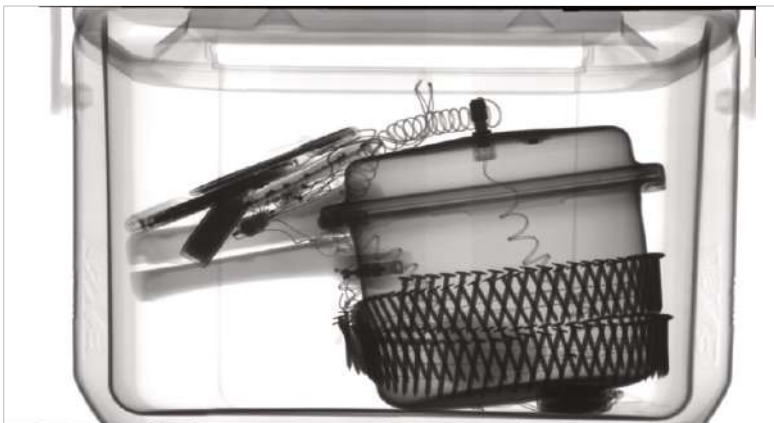
Image 1



Image 2

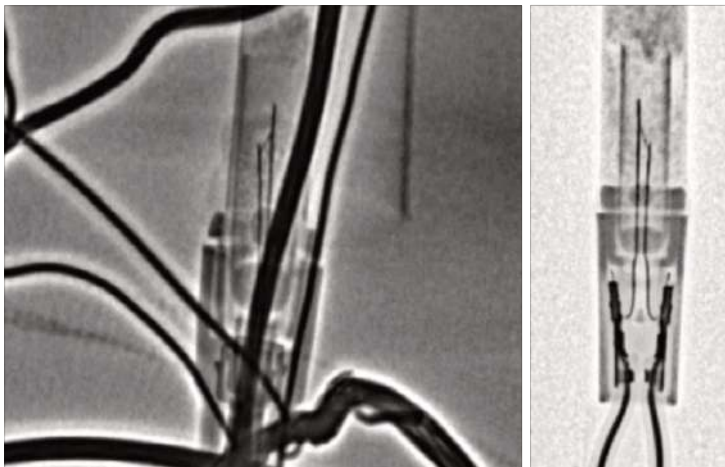


Image 3



Stitched Image

Zooming and magnification are crucial for identifying and understanding explosive devices. To achieve magnification, the operator must position the detector at a specific distance from the package. A key factor in this process is the X-Ray source's focal spot; a smaller focal spot is essential for producing clear, readable images. The Teledyne ICM battery-operated generators, including models CP120B, CP160B, and LITEX, provide an ideal solution.



Time is also a critical factor for EOD operators, who must secure areas swiftly to ensure public safety. Teledyne has prioritized this need in its product designs, aiming to quickly determine whether a package poses a threat. Consequently, Teledyne ICM

innovative team introduced the C-View, a Live Video X-ray imaging system that enables rapid assessment of packages within seconds. Being operational in under 90 seconds, this solution is ideal for time-sensitive operations. ■



ABOUT TELEDYNE ICM

Teledyne ICM has over 25 years of expertise in developing innovative portable radiography solutions. Its portable generators have excellent technical capabilities and when coupled with high-resolution detectors, provide highly accurate radiographs. Contact: icm.sales@teledyne.com

THE LOUDEST MESSAGE: DETONATION OF COMMUNICATION DEVICES IN LEBANON

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

"The death of communication is the birth of resentment."

(From Dave Ramsey's online broadcast show, 12 April 2012)

One of the most effective tactics, techniques and procedures conducted by several Palestinian militias in support to the attacks carried out in Gaza last October 2023 was based on the use of personal mobile radios (also called "walkie talkies") and other, more secure than mobile phones, communication devices for obtaining information and ensuring the security of operations.

On 17th September 2024, at about 15:30 local time (12:30 GMT), the simultaneous detonation of more than 2000 handheld pagers/beepers was reported in Lebanon (e.g. Beirut, Tyre) and even in Syria; those devices were acquired by the Hezbollah organization.

On 18th September 2024, the detonation of more than 400 electronic devices of another kind (mostly personal mobile radios (PMR), as well as detonations of laptops, video cameras, mobile phones, solar energy equipment, biometric identification systems...) under Hezbollah's ownership were also reported in Lebanon.



Figure 1: Geographical allocation of the reported detonations of pagers.
(Source - www.abc.es)

Buzzing hazards: controlled detonation of Hezbollah's personal pagers

The referred pagers were acquired by the Hezbollah group at the direction and guidance of their leader, who ordered the move from the use of mobile phones to more secure means, with the aim of avoiding the evidenced tracking of Hezbollah members by Israeli intelligence services; accordingly, Hezbollah ordered about 5000 pagers late 2023 or early 2024.

The model of the detonated pagers is identified as the "AR-924 RUGGED PAGER" by the Taiwanese company GOLD APOLLO LTD.

The technical characteristics and capabilities of the RUGGED PAGER AR-924 are as follows:

- It is PC-programmable and hand-programmable, 4 buttons with two-way scrolling, and a 4 lines LCD screen (LCD 164 x 64 pixels, 64 points per inch).
- It can store up to 30 messages with a maximum length of 100 characters. Its data transfer rate is 512/1200/2400 bit/s for POCSAG.
- Dimensions are 73 mm x 50 mm x 27 mm (2.9 in x 2.0 in x 1.1 in), and weight is 133 g (4.7 oz).
- It has a removable Li-ion battery, rechargeable via a USB-C connector, and lasting up to 85 days with 2.5 hours of charging.



Figure 2: Pictures of the post-blast remains from pagers showing details about the company and model. (Source: X)

Rugged Pager AR924

IP67 Dust and Waterproof

Up to 85 Days of Battery Life

Rechargeable battery with USB-C connector



Figure 3: Images from GOLD APOLLO Rugged Pager AR-924. (Source: GOLD APOLLO LTD.)

After the technical analysis of the effects (taken from the available photographs), we could estimate that:

- The detonation appears to have started from inside the battery or even near the battery on its inner side surface (see how the metal battery cover folds from the inside out).
- Although thermal deformation of the plastic is evident, it could be also produced due to a previous

detonation and once the battery cover is broken/penetrated and the inner battery chemicals react with oxygen, which could produce combustion and even deflagration.

- The overall effects initially seem too severe from a single battery overheating, consequent production of gases, and final detonation by the convergence of overpressure and temperature conditions.



Figure 4: Images allegedly taken from GOLD APOLLO Rugged Pager AR-924 remains. (Source: X)

As stated by witnesses, the pager detonation took place some seconds after receiving a specific message, so that the user has enough time to pick up the pager and bring it to their eyes for reading. Along with the previous months of use of the pagers, this pattern points to some kind of software pre-programming on the motherboard that, after receiving the certain signal, causes the battery to overheat (and prevent the motherboard's electronic monitoring/temperature from rising to a critical point) and/or produces an electrical signal, that initiates the detonator.

Open sources' reports are pointing at two different origins of detonation, such as:

- Extreme overheating of the battery, and consequent detonation of it.
- Detonation of the embedded pentaerythritol tetranitrate (PETN) due to severe overheating of the battery in close contact with this explosive substance.

If we comprehensively analyze the photographs and videos showing the effects of explosions on victims, the overheating of the battery unit before detonation due to gas release, burning, and overpressure on the metallic container of the battery is not consistent with the disruptive, breaking, and penetrating injuries resulting from the explosion, and the expected burn effect on human skin and clothing is not evident.

On the other hand, and from the technical perspective, PETN is an explosive which:

- Is very powerful (1.6 relative effectiveness as compared with Trinitrotoluene TNT), which makes its use compatible with the observed high effects with a small amount of explosive.
- Although PETN has a relative sensitivity to heat and detonation, in principle, it would need a detonator to start the detonation process.
- Although PETN has an impact sensitivity of 3-4 J and a friction sensitivity of about 60 N in the dry state, these conditions are very difficult to achieve inside small electronic devices such as pagers.
- When exposed to high temperatures (such as severe overheating of a battery), PETN melts and

enters a state of reduced sensitivity, making the melted PETN unable to detonate even with a detonator (re-solidification is required to restore sensitivity to the action of a detonator). To make it sensitive to heat, PETN must be mixed with another, more sensitive explosive.

- Could be initiated by laser pulse (but this would require a directed pulse to each device, which is not consistent with the simultaneous detonation of hundreds of devices).
- Nonetheless, PETN is sensitive to an electrical spark with a range of 10 to 60 mJ, or even by creating an exploding wire detonator or exploding foil initiator (no primary explosives are needed for detonation due to the vaporization of the metallic bridge-wire and the subsequent plasma shock and heat that will cause PETN to detonate), but this would require a high voltage, high current, low impedance electrical source, which a pager apparently cannot provide.
- In principle, PETN is more difficult to detect than other explosives due to its lower vapor pressure.

Last call to hell: controlled detonation of Hezbollah's personal mobile radios

With regard to the detonation of personal mobile radios (PMRs or walkie-talkies) in Lebanon, the model is identified as ICOM IC V-82.

It is believed that the detonation was caused by a battery, and although it appears that the detonation was more powerful than the pagers and the effects on the victims caused many more deaths in comparison, the effects on the body of PMRs are not very high in most of the observed cases.

Since it appears that not too many PMRs detonated and the cause was the battery, it is initially assumed that the portable radios may have exploded due to a modification of the spare batteries, as well as due to the reception of a certain code.

Taking into account the limited information available from open sources and from quick indirect analysis, it appears that the electronic communication devices may have been detonated through:



Figure 5: Images allegedly taken from the referred PMR's remains. (Source: X)

- Reprogramming the devices anywhere during the logistic movement from factory to client.
- Modification of the electronics, which would create an additional circuit for detonation.
- Receiving a message that includes a specific coded order.
- Adding a small amount of an explosive (maybe 05-10 grams if PETN-based, depending on the available space inside the pager) along with a secondary circuit with a thyristor/transistor plus a micro-detonator or simply an explosive mixture capable of being initiated by flame/heat.

Actions and effects

This is not the first time that commercial off-the-shelf (COTS) personal electronic devices have been manipulated to become improvised explosive devices; however, it is the first documented instance of this technique being used on a massive, semi-indiscriminately, and simultaneous basis against an adversary organization.

The coordinated detonation of electronic communications devices would not only result in deaths and injuries among Hezbollah personnel, but would also seriously impact internal



Figure 6: Images of other kinds of electronic devices allegedly affected by detonations in Lebanon. (Source: X)

communications and coordination capabilities among Hezbollah members.

The responsibility for the attacks have not been officially claimed yet, but the author of the attacks sends an implicit message to Hezbollah about the author's capabilities, his agility and versatility, and highlights Hezbollah's vulnerabilities.■

*"Let your plans be dark and impenetrable as night,
and when you move, fall like a thunderbolt."*

(Sun Tzu, in his book "The Art of War"
allegedly first published in 401 BC)

REFERENCES

- X (former TWITTER)
- TELEGRAM
- VKontakte (VK)
- www.abc.es
- www.telex.hu
- www.youtube.com/watch?app=desktop&v=x50wwGjX2Ao
- www.doi.org/10.1002/prep.202200150
- www.rigpix.com/icom/icv82.htm
- www.gapollo.com.tw
- www.rfsafe.com
- www.dailymail.co.uk
- www.washingtonpost.com

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 the 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



HOUTHI USV WBIED ATTACKS TARGETING MERCHANT SHIPS IN THE RED SEA, YEMEN

By Chief Superintendent (ret.) Michael Cardash, Terrogeance - Global

On June 12, 2024, the Liberian-flagged, Greek-owned bulk carrier M/V Tutor was targeted in the Red Sea by two unmanned surface vessel water-borne IEDs, forcing the crew to abandon ship a few days later and resulting in the ship's sinking. The Houthis claimed responsibility for the attack one week after it was carried out.

Though unmanned WBIED attacks have been previously reported, this appears to be the first documented attack of a Houthi USV WBIED against a ship in the Red Sea since October 2023, the start of the Toufan Al-Aqsa / Iron Swords War in the Gaza Strip between the State of Israel and the Palestinian armed groups led by Hamas.

ANALYSIS

According to reports, the attack occurred about 66 NM (nautical miles) southwest of the Houthi-controlled port city of Al-Hodeidah, closer to the African coast of the Red Sea. The Tutor had completed a port call in Russia and was bound for Egypt, when it was struck in the stern by "a small, white-colored craft" with an estimated length of 5-7 meters, occupied by two mannequins. The subsequent impact and explosion caused severe flooding and damage to the engine room, leaving the Tutor unable to maneuver.



A USV WBIED approaching the Tutor



The USV WBIED and its two mannequins

The Houthis claimed responsibility for the attack on the same day it took place, stating Tutor was targeted using a USV WBIED, as well as “several UAVs and ballistic missiles.” In another statement released on June 15, 2024, Houthi military spokesman Yahya Sari asserted the Tutor was “expected to sink in the coming hours” and stated the

attack was part of the escalation measures in support of the Palestinians in Gaza against the backdrop of the Toufan Al-Aqsa War. On June 19, 2024, the Houthis released a short video documenting the attack on the Tutor, which reportedly involved the use of two USV WBIEDs and what seems to be additional missiles.



The attack by the first USV WBIED



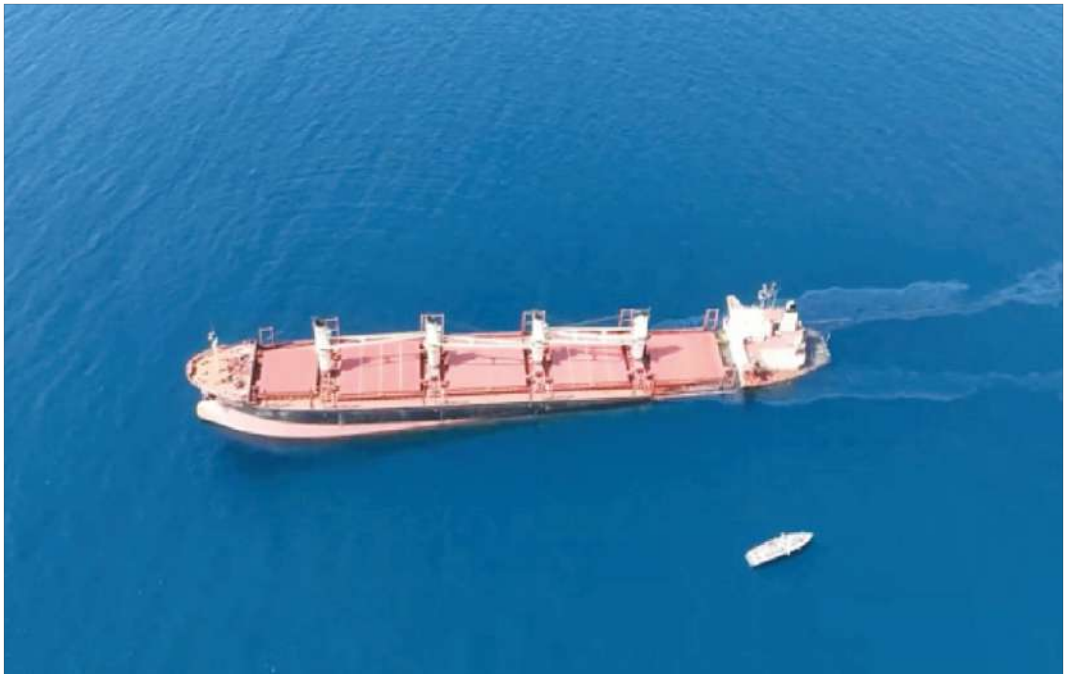
The attack by the second USV WBIED



Impacts by at least three missiles as well

The following weekend, between June 14 and 15, 2024, the crew abandoned ship and was airlifted by the USS Dwight D. Eisenhower Carrier Strike Group. According to a statement by US White House National

Security Communications Advisor John Kirby, one Filipino crew member was killed in the attack and a Sri Lankan sailor was critically wounded. The ship was abandoned and eventually sank in the Red Sea.



The ship before it sank



The ship taking on water before it sank

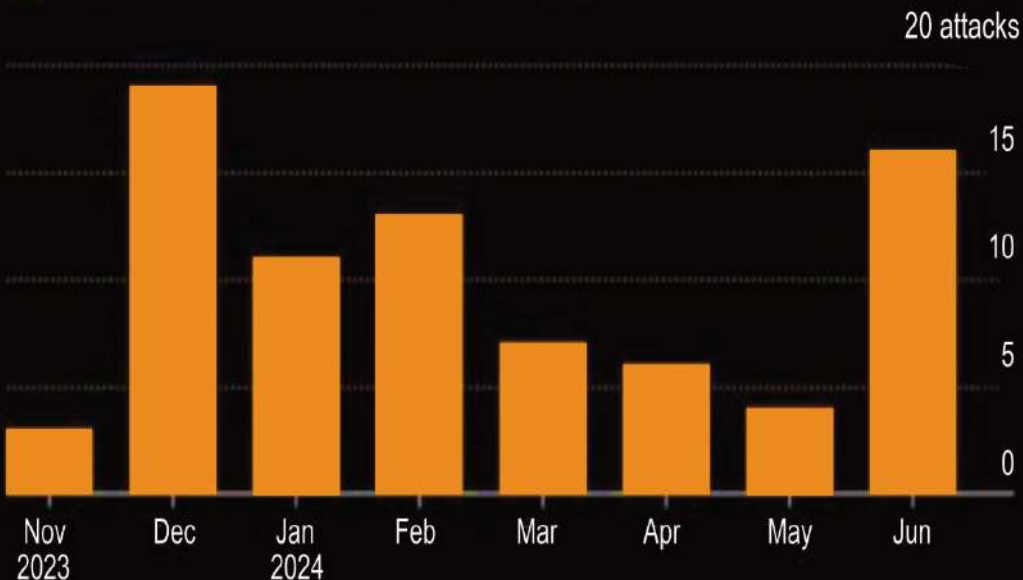


Crew members airlifted to safety

Houthi Ship Attacks on the Rise Again

June was the busiest month of incidents this year

■ Attacks on vessels in the Red Sea and Gulf of Aden



Source: JMIC

Bloomberg

Houthi maritime attacks against vessels, November 2023 - June 2024

ASSESSMENT

From the early stages of the Toufan Al-Aqsa (“Al-Aqsa Flood”) / Iron Swords War, which started in the Gaza Strip on October 7, 2023, with a large-scale surprise attack against Israel led by Hamas, the Yemen-based Houthi (Ansar Allah) movement has associated itself with the fighting in several phases of escalating actions “in solidarity with and support of the oppressed Palestinian people.”

According to analysts and observers, during the first half of 2024, the Ansar Allah movement carried out 57 attacks against vessels, and a total of 79

attacks since November 2023 (see the diagram above). However, other statistics suggested higher numbers, which likely include unconfirmed or unofficial attacks, as well as attacks that targeted the same vessel more than once.

The Houthis’ use of USVs is not new and has been documented since 2017, first to attack military vessels belonging to the Saudi-led coalition, such as in the attack on the Saudi frigate Al Medina in January 2017, and the attempted attack on the British HMS Duncan in July 2019, and then against oil tankers in 2020.



The Saudi frigate Al Medina targeted in January 2017



Saudi tanker Gladiolus targeted in March 2020

During this period, three types of USV WBIED platforms were documented in use by the Houthis:

- Shark-33 (a patrol boat modified for use as an USV WBIED)
- Blowfish (a dedicated USV WBIED)
- Fishing boats (USV WBIEDs disguised as fishing boats)



Shark-33 USV WBIED (top and center) with an SS-N-2 Styx anti-ship missile warhead (bottom)



المركز الإعلامي للمنطقة العسكرية الخامسة
Media Center of the Fifth Military Region



المركز الإعلامي للمنطقة العسكرية الخامسة
Media Center of the Fifth Military Region



المركز الإعلامي للمنطقة العسكرية الخامسة
Media Center of the Fifth Military Region

Blowfish USV WBIED

	Shark-33 modified 10-meter patrol boat	Blowfish USV WBİED
Length	10 meters	5.82 meters
Width (beam)	2.30 meters	2.44 meters
Height above sea level	-	1.5 meters
Cruising speed	35 knots	-
Maximum speed	45 knots	30
Propulsion	2 x 200hp L200A Yamaha outboard motors with 165 US gallons of fuel	1 x 200hp Yamaha outboard motor
Explosive charge	Warhead of a Soviet P-15 Termit anti-ship missile (SS-N-2 Styx) – 454 kg hollow charge HE	Unknown quantity of HE
Guidance and monitoring	Garmin GPS antenna, Nexus 35° autopilot compass, remotely operated video camera	GPS device

As stated, the third model documented in the past is a fishing boat (skiff,) used mainly for the purpose of camouflage, containing an explosive payload previously documented as a box containing explosives, and later, as a metal barrel with an EFP warhead configuration. In our estimation, this type of boat was used in the attack against the Saudi tanker *Gladiolus* in March 2020, as well as against the *M/V Tutor* in June 2024.

On January 18, 2024, Project Masam - a Saudi humanitarian landmine clearance project in Yemen - recovered a USV WBİED previously used by the Houthis to target international shipping boats in the Red Sea.

The WBİED consisted of a basic blue wooden boat resembling numerous civilian fishing boats that sail along the Red Sea coast every day, which was found unmanned and floating near the coastal Bab al-Mandab village, southwest of the Murad area, where

fishermen dragged it back to shore. It was left untouched for a month among other fishing boats. With no one claiming the boat, local villagers decided to inspect the vessel and spotted wires protruding from a hole in the hull of the boat, and they subsequently reported it to Project Masam.

After investigating the boat, bomb disposal technicians discovered the wires led to a large explosive payload hidden in a large container under the deck in the hull. It reportedly consisted of 25 kg of C-4 explosives and at least 50 kg of TNT, as well as 20-25 liters of gasoline in containers.

According to Project Masam bomb disposal experts, the warhead had an EFP configuration, and was identified as a Houthi IED.

It has been estimated the USV WBİED was sent from Houthi-occupied port city Al-Hodeidah and was RC-controlled to sail along the coast toward Bab al-Mandab.



The fishing boat



The payload (left) with an EFP warhead (right)

On September 21, 2022, the Houthis unveiled, for the first time, during a military parade in Sana'a three types of USV WBIEDs, designated "Toufan" class USVs.

All three models have cockpits, arches, antennas, and a waterjet motor for propulsion. The Toufan-2 seems to have a glass dome camera and the Toufan-3 incorporates a different type of camera, possibly some

type of a maritime forward-looking infrared (FLIR.) The Toufan-3 also has a Simrad HALO dome radar on its arch and in the lower part of the arch, another smaller white color dome component - possibly an autopilot compass.

In the Toufan-1, there is a single seat for one person, while the Toufan-2 and Toufan-3 have two seats, one behind the other.



Toufan-1



Toufan-2



Toufan-3

Comparison of technical info provided by the Houthis:

	Toufan-1	Toufan-2	Toufan-3
Warhead mass (kg)	150	400	500
Speed (knots)	35	41	52
Range and targets	Close range sea targets, stationary and mobile	Stationary and mobile sea targets	Far range sea targets, stationary and mobile

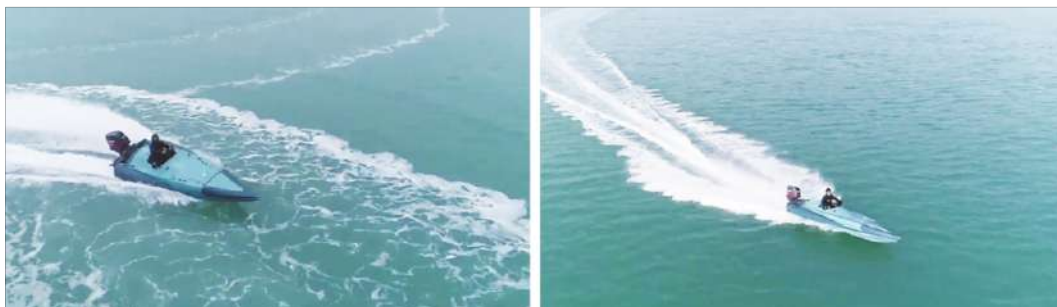
On June 21, 2024, the Houthis released a video in which they revealed information and documented their testing of the Toufan-1 USV WBIED. The video shows a boat that can be steered either manually or by RC control, targeting “a naval target” (a vessel) at sea.

Specifications of the Toufan-1, per the Houthi video:

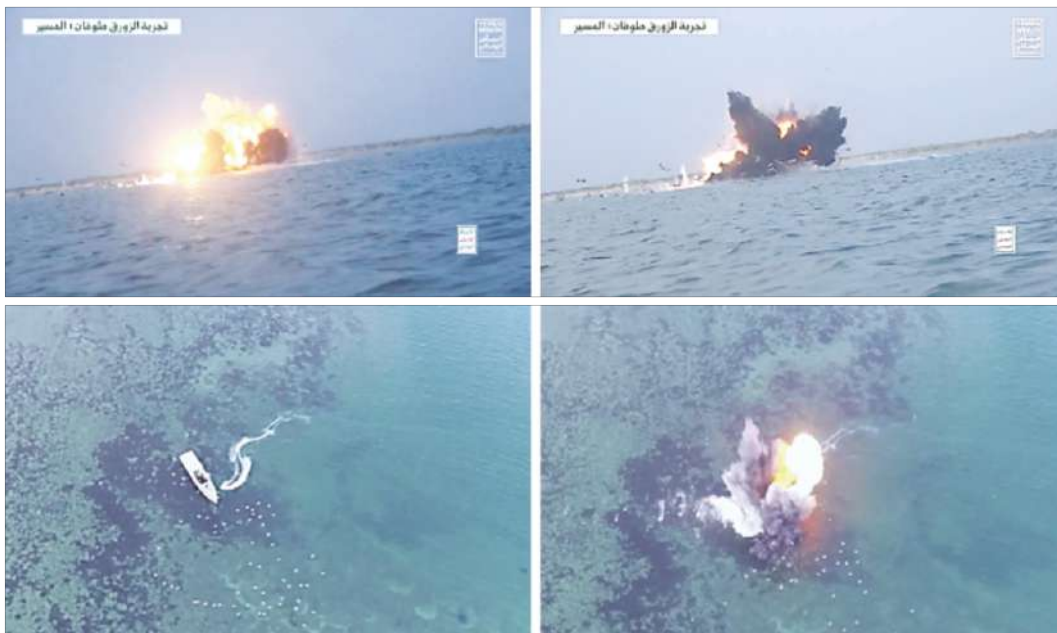
- A locally produced USV WBIED capable of reaching high speed, maneuvering stealthily, and targeting close-range naval targets, both mobile and immobile
- Explosive payload (warhead): 150 kg
- Speed: 35 NM/h



Toufan-1



Toufan-1 with manual steering



Toufan-1 with RC-control steering in a test attack against a boat



A closer look at the results of the test attack

Toufan al-Mudammir (Lit. “Destructive Toufan,” an improved Toufan-3)

On the evening of June 21, 2024, the Liberian-flagged Greek-owned bulk carrier M/V Transworld Navigator was attacked in the Gulf of Aden, 126 NM east of Aden city, while en route from Malaysia to Egypt. Explosions were witnessed in the vicinity of the vessel, which proceeded to its next port of call. The following day, the Houthis claimed responsibility for the attack, stating it involved the use of “ballistic missiles” against the vessel.

On June 23, 2024, the Transworld Navigator was targeted again by the Houthis, 65 NM west of Al-Hodeidah, off western Yemen’s coast, using a USV WBIED. The Houthis claimed responsibility for this attack as well. Documentation showed moderate

damage was caused to the ship, with minor injuries reported as well by the US Central Command (US CENTCOM.) A USV approaching the vessel was also documented on video.

On June 30, 2024, the Houthis published a two-part video documentation of their new Toufan al-Mudammir. The first part documents the targeting of the Transworld Navigator with a Toufan al-Mudammir USV WBIED. Of note, the first frame of this part includes footage taken by a camera positioned on the bow of the USV. The second part of the video documents the testing of the USV WBIED at sea, which includes maneuvering between buoys. The testing covered both manual and RC-controlled steering, the latter ostensibly possible only at a limited range. The Houthis published the specifications of the new Toufan.



The USV WBIED reaches the Transworld Navigator attack

Toufan al-Mudammir specifications:

- Locally produced offensive USV with high destructive power
- Warhead: 1,000-1,500 kg
- Speed: 45 nautical miles per hour



Attack targeting the Transworld Navigator with a Houthi Toufan al-Mudammir USV WBIED



Toufan al-Mudammir with manual steering



Toufan al-Mudammir with RC-controlled steering

Specification	Toufan al-Mudammir	Toufan-3
Warhead	1,000-1,500 kg	500 kg
Speed	45 NM/h	52 NM/h

The array of weapons in the possession of the Houthis that threaten the shipping lanes in the Red Sea include surface(coast)-to-sea missiles, cruise missiles, ballistic missiles, UAVs, and a wide variety of USV WBIEDs.

The advantages of the USVs are mainly in their ability to accurately hit the targeted ships, especially since they are controlled using cameras located in the bow of the vessels.

Of note, the use of sailing vessels disguised as fishing boats with mannequins propped up in them is intended to prevent the vessel from being destroyed at a distance from the target, by creating confusion and doubt among the defending forces onboard the target as to whether the boat is on an offensive or innocent mission. ■

ABOUT THE AUTHOR



Chief Superintendent (ret.) Michael Cardash, Senior bomb technician and former deputy head of the Israeli police bomb disposal division, commanded bomb disposal units within the border guards and police during intense terrorist conflicts in Israel. Michael currently is the senior

CIED analyst at Terrogence-Global, IED's and authors the Terogence Möbius C-IED reports analyzing and assessing global IED-related technical and tactical intelligence.



22 - 26 OCTOBER 2024
ISTANBUL EXPO CENTER



SECRETARIAT OF
DEFENCE INDUSTRIES

ISTANBUL
CHAMBER OF
COMMERCE

İSTANBUL
CHAMBER
OF INDUSTRY

THIS EXHIBITION IS ORGANIZED WITH THE AUDIT OF TOBB (THE UNION OF CHAMBERS AND COMMODITY EXCHANGES OF TURKEY) IN ACCORDANCE WITH THE LAW NO.5174.

“SAMBA JIHAD”: SOCIAL MEDIA, EXPLOSIVES AND DAESH FOLLOWERS IN SOUTH AMERICA

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

“The fools. But just because they are fools does not mean they are not a threat.”

(Kendare Blake in her book “Three Dark Crowns”, first published in 2016)

On March 17, 1992, the Islamic Jihad Organization ordered a suicide driver in a pick-up vehicle loaded with explosives (VBIED) to attack the Israeli Embassy in Buenos Aires: not only were 29 persons killed and another 242 more were wounded, but it also destroyed the embassy, a Catholic church, and a nearby school building.

On July 16, 1994, a suicide bomber attack on a Panamanian commuter plane killed all 21 people on board. Investigators identified the attack as the work of Jamal Lya, a Lebanese citizen using fraudulently obtained Colombian documents and believed to be working for Hezbollah.

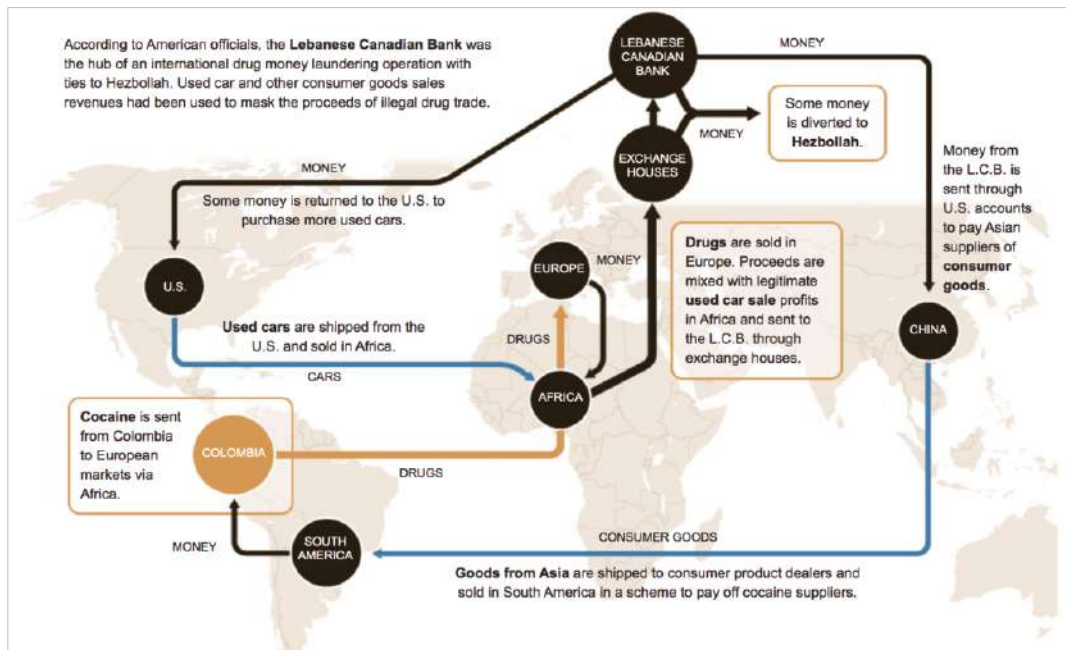


Figure 1: Worldwide money laundering network as used by Hezbollah organization in the past. (Source - The New York Times)

On July 18, 1994, a Vehicle-Borne Improvised Explosive Device (VBIED) was detonated beside the Argentine Mutual Israelite Association (AMIA) Jewish community center building in Buenos Aires, killing 85 people and injuring hundreds.

The development of human networks supporting both Hezbollah and Iran in South America has been well known, but in recent years we have seen a growing presence of jihadist activists/supporters scattered throughout the Latin American region.

DAESH joined the South American TELEGRAM terror league

A TELEGRAM channel ("https://t.me/UtinamArchivo") was created on January 2, 2024, by two Brazilian citizens.

"*Utinam*" is an old Latin term freely translated as "a fervent wish", while the Portuguese term "*Arquivo*" means "archive"; the referenced and private TELEGRAM channel was a huge repository of training documents and videos about several topics indirectly connected with survival tactics and even subversion through several sub-channels as listed below:

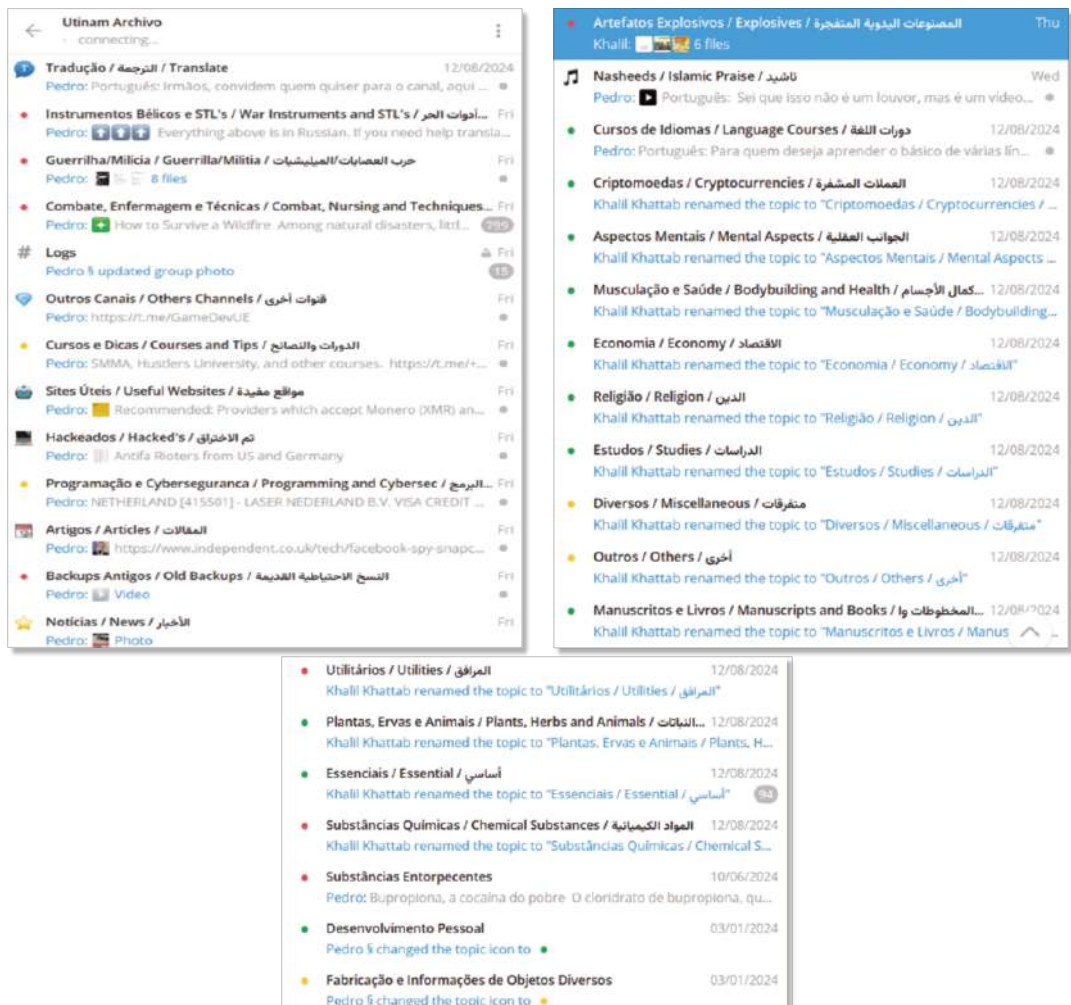


Figure 2: Information about the referenced channel and its sub-channels sharing instructional files. (Source: Telegram)

Among other topics rated as potentially less risky were some sub-channels that effectively exchanged instructional information (mostly in English and translated into Portuguese, but also in Ukrainian and Russian) about:

- Explosives and IEDs
- Improvised weapons and 3D-printed firearms
- Jihadist propaganda
- Chemical agents
- Narcotics

It was on August 1, 2024 that the leaders of the aforementioned TELEGRAM channel (along with a clear demonstration of loyalty to DAESH) began to openly share information containing propaganda and documents:

- **DAESH videos with English subtitles and manuals (by Al-Saqri Foundation for Military Sciences) on homemade explosives and IED manufacture.**



Figure 3: Shared DAESH videos and (translated) manuals on homemade explosive manufacture. (Source: Telegram)

- DAESH propaganda



Figure 4: DAESH propaganda through “Utinam Archivo” channel.

(Source: Telegram)

As a result of repeated complaints about its “terrorism-supportive” content, the TELEGRAM channel “Utinam Archivo” was banned last August, although most of its members remain active on social media.

Opening Jihadi influence borders: Iberian languages overlap Arabic and English ones

Jihadist forums and social media (e.g. RocketChat) are showing a growing presence of Portuguese and Spanish languages around the propaganda machinery.

One of the oldest channels on RocketChat, aimed at South American and Spanish subscribers, is “#Fursan_al_Tarjuma_Voz_de_al_Andalus”, which primarily shares DAESH news, pictures and videos translated into Spanish. This is all part of a larger effort to publish in different languages from the DAESH-related “Fursan al Tarjuma” (translates as “Knights of Translation”) propaganda franchise.

But another channel using the Spanish language (#AlAndalus) has been recently created by a DAESH follower in Uruguay (4th September 2024), which is sharing videos (including one filmed and distributed by the perpetrators of the 2017 Barcelona attacks), news about the activities of South American DAESH followers, and even quite basic recommendations for using gas cylinders as the main charge during attacks.

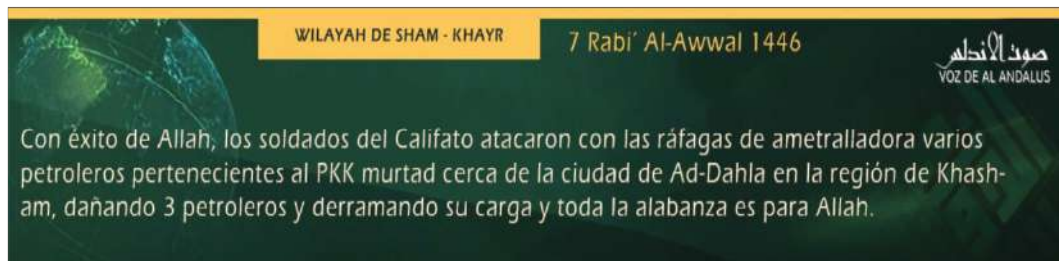


Figure 5: Information shared by “#Fursan_al_Tarjuma_Voz_de_al_Andalus” channel. (Source: X)



Figure 6: Information and capture from a shared video by “#AlAndalus” channel. (Source: RocketChat)

The members of those channels appear to be connecting from Brazil, Uruguay, Argentina, and Spain.

Another dedicated channel (#COMANDO_860) for South American DAESH followers was created on September 11, 2024 (the 23rd anniversary of the 9/11 attacks), by another user who identified himself as a Brazilian citizen; the first file shared through the channel was a kind of pledge of allegiance (Bayat) to DAESH.



Figure 7: Badge of “COMANDO 860” group. (Source: X)

Among other topics such as survival manuals, documents on radical ideology, DAESH propaganda (videos, posters, pamphlets... including the re-distribution of a video calling for an attack on infidels using explosives, “*You have to deal with them, O monotheist*” by DAESH Ar Raqqa media office). The channel also shares a Brazilian-language version of the explosives handbook published by Al-Saqri Foundation for Military Sciences.

“Trick or Treat”: some conclusions about jihadism in South America

With regard to the dissemination of manuals for homemade explosives (HMEs) and improvised explosive devices (IEDs) through the previously mentioned forums and channels, the technical instructions contained in some documents are considered as effective and reliable in terms of HME, IEDs, and even improvised firearms including 3D-printed ones.

Although DAESH followers in Iberian America are not limited to the initiatives described above, it is certainly evident that Brazilian elements are more active in terms of propaganda, calls for action and training instructions in weapons and tactics.

The growing online activity of DAESH followers inside Brazil and other South American countries could be a potential indicator of planning of further

violent actions against Christian and Jewish targets, with a higher likelihood of interest in the United States as a target.

Taking into account the current dynamics of online activity by South American DAESH followers and the lack of a solution to the conflict involving Israel, Palestine and Lebanon, continued growth in efforts by South American DAESH followers and even future fighters is likely. ■

“Quem não arrisca não petisca”
(Those who don’t take a risk don’t have a snack.)
(Brazilian traditional quote)

REFERENCES

- X (former TWITTER)
- TELEGRAM
- RocketChat
- ÁLVAREZ, PEDRO TRUJILLO. *“Presencia Del Terrorismo Yihadista En América Latina.” Cuadernos de Pensamiento Político*, no. 59 (2018): 77–86. <https://www.jstor.org/stable/26482884>.
- MARULANDA, JOHN. *“Yihad en Latinoamérica”* (EDC DIPON / EDC GATO AZUL, 2016)
- www.fdd.org/analysis/2020/08/04/crisis-in-lebanon/

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 the 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

Defense & Security 2025



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
f Defense and Security 2025
in Defense Security Thailand
globe asiandefense.com

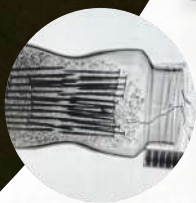
Organised by:



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



X-ray Systems designed and built for bomb techs