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

Counter-IED Report

Winter 2016/17

CHANGES IN THE COUNTER–IED OPERATIONAL ENVIRONMENT

C-IED EDUCATION AND TRAINING – THE WAY FORWARD

THE ISLAMIC STATE IN IRAQ AND SYRIA IED REVOLUTION

FAKE BOMB SEARCHERS:
EXPLOSIVE DETECTION SCAM IS SCARING THE C-IED MARKET!

EXPLOSIVES TRACE DETECTION:
CRITICAL COMPARISON OF TECHNOLOGICAL SOLUTIONS FOR OPERATORS

DENSITY RANGES OF EXPLOSIVES FOR
DEVELOPING X-RAY DETECTION WINDOWS

IEDs: ATTACK THE NETWORKS –
NEED FOR MULTI-AGENCY COORDINATED EFFORT

WEAPONS EXPLOITATION AND POST BLAST
SCENE INVESTIGATION TRAINING

CONTENTS

IFC QINETIQ NORTH AMERICA

4 - 5 GARRETT METAL DETECTORS

7 ICOR TECHNOLOGY

9 THERMO FISHER SCIENTIFIC

11 DSA DETECTION

12 PRIMETECH - A DIVISION OF FAE GROUP S.P.A.

12 SERIM RESEARCH CORPORATION

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

15 HARRIS CORPORATION

16 BBI DETECTION

16 ISDEF EXPO 2017

17 CHANGES IN THE COUNTER–IED OPERATIONAL ENVIRONMENT
By Russell McIntyre, former US Department of Defense

23 MILITARY ENGINEERING 2017

24 BORDER MANAGEMENT & TECHNOLOGIES SUMMIT 2017

CONTENTS

25 **C-IED EDUCATION AND TRAINING – THE WAY FORWARD**
By Torsten Gottlieb, Lieutenant Colonel DEU Army, Branch Chief
Philippe Belda, Lieutenant Colonel FRA Army, Lessons Learned Section Chief
Jose Lopez Navarro, Lieutenant Commander ESP Navy, Training Section Chief
Dragos Gheorghe, Major ROU Army, R&D Analyst within LL section
Niklas Tornesjo, Lieutenant Colonel SWE Army, Exercise Coordinator Training Section
Levente TÁBI, Lieutenant Colonel, Hungarian Army / Engineer Corps

33 **SECURITY & COUNTER TERROR EXPO 2017**

34 **NCT ASIA & SISPAT SINGAPORE 2017**

35 **THE ISLAMIC STATE IN IRAQ AND SYRIA IED REVOLUTION**
By Greg Robin - Sahan C-IED Expert, Camille Chautard - Sahan Analyst and
Stephanie Braquehais, Editor

41 **DSEI 2017**

42 **13th INTERNATIONAL DEFENCE INDUSTRY FAIR - IDEF 2017**

43 **FAKE BOMB SEARCHERS: EXPLOSIVE DETECTION SCAM IS SCARING THE C-IED MARKET!**
By Lieutenant Colonel Jose M Rufas, Head of the Defeat the Device Branch,
C-IED Centre of Excellence

49 **CBRNe SUMMIT EUROPE 2017**

50 **ISDEF EXPO 2017**

CONTENTS

51 EXPLOSIVES TRACE DETECTION: CRITICAL COMPARISON OF TECHNOLOGICAL SOLUTIONS FOR OPERATORS
By Simon O. Williams, BA, LLM, Managing Director, Tactique Services

56 DENSITY RANGES OF EXPLOSIVES FOR DEVELOPING X-RAY DETECTION WINDOWS
By John D. Howell, DSA Detection

61 CBRN INTERNATIONAL 2017

62 UNDERSEA DEFENCE TECHNOLOGY – UDT 2017

63 IEDs: ATTACK THE NETWORKS - NEED FOR MULTI-AGENCY COORDINATED EFFORT
By Colonel H R Naidu Gade (Retd.)

70 MILIPOL ASIA-PACIFIC 2017

71 WEAPONS EXPLOITATION AND POST BLAST SCENE INVESTIGATION TRAINING
By Robert Shaw, Security and Intelligence consultant

75 BIDEC – BAHRAIN INTERNATIONAL DEFENCE EXHIBITION & CONFERENCE

76 POWERING THE THREAT: IMPROVISED BATTERIES FOR PORTABLE ANTI-AIRCRAFT MISSILES
By Lieutenant Colonel Jose M Rufas, Head of the Defeat the Device Branch, C-IED Centre of Excellence

OBC SCANNA MSC LTD

FOREWORD

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

2016 witnessed a continuing growth in terrorism and insurgency across the globe. The countries currently of particular interest in which the West and other nations have been recently actively engaged – Afghanistan, Iraq, Libya and Syria - all continue to be characterised by violent Islamist insurgency and civil war. Afghanistan presents severe problems long after the Coalition forces have, in the main, left the country. The central government in Kabul does not yet have firm governance across the nation and the Taliban and ISIS continue to exploit this tenuous security environment. Afghanistan remains the world's major producer of opium and recently the United Nations announced that production had increased by 43% over the past year. This is despite major Western efforts to eradicate opium production over the past ten years. In Iraq, the military have met with some success during 2016 after years of setbacks. In June Iraqi forces, heavily backed by US airstrikes, recaptured the key city of Fallujah from ISIS fighters. As 2016 drew to a close the Iraqi forces are heavily engaged in efforts to retake Iraq's second city, Mosul, having lost it to ISIS in 2014. Prior to the Iraqi assault on Mosul, ISIS had ample time to prepare defensive positions in which IEDs are playing a devastating role. Again, Coalition airstrikes are impacting on ISIS capabilities significantly, though in the built up areas of Mosul, airstrikes are more problematic and ISIS exploit this situation by the rapid use of Vehicle Borne IEDs. Libya remains a dysfunctional and lawless country which poses an existential problem for Europe in terms of migrants attempting to cross the Mediterranean to southern Europe. 2016 saw a record number of people – more than 180,000 attempting this route and this has resulted in at least 5000 deaths by drowning. ISIS continues to gain influence in Libya. Syria witnessed major conflict throughout 2016 and this culminated in December with the recapture of Aleppo by the Assad regime with major support from Russia and Iran. The world looked on helplessly as the humanitarian situation in Aleppo during and after the fighting reached catastrophic proportions with tens of thousands of civilians fleeing the war ravaged city. It is estimated that up to one million people have died as a result of the war in Syria between 2011 and 2016.

Sahan Research provides a very sobering and insightful assessment of the technical and manufacturing skills of ISIS IED production in Iraq and Syria. The Iraqi Army assault to regain Mosul from ISIS is currently being severely hampered by the insurgents' widespread use of IEDs both offensively and defensively. A particularly worrying discovery by Sahan is that of the ISIS manufactured anti-vehicle and anti-personnel Victim Operated Directional Fragmentation Charge – a device that demonstrates high level technical and manufacturing skills. ISIS is currently exporting its IED making skills to other insurgencies – Libya being a case in point. Sahan reinforces the urgent need for International Humanitarian Law to recognise IEDs for what they are - specialised mass produced weapons that indiscriminately target civilians.

Lieutenant Colonel Torsten Gottlieb and his staff from the NATO C-IED Centre of Excellence (COE) which is located in the western part of Madrid and opened in 2010 provide a most comprehensive description of this critically important organisation. As evidenced in the

recent conflicts in Afghanistan and Iraq, the IED was the main existential threat to the safety and security of NATO personnel – a threat that has only increased in recent times. The stated mission of this COE ".... is to provide subject matter expertise in order to support the Alliance, its Partners and the International Community in the fight against IEDs." The article describes the research, training courses and field exercises conducted by the Centre and also the vital function of recording lessons learned.

Robert Shaw examines the critical importance of Weapons Exploitation and Post Blast Scene Investigation Training in the fight against IEDs. He points out that the activity that links the short term force protection element of IEDD and long term element of attacking the networks is Post Blast Scene Investigation – also known as Weapons Exploitation – carried out by police scenes of crime officers or military weapons exploitation teams. He describes the composition and skills of a typical team, the requisite training for the team and the necessary TTPs.

In a second article from the NATO C-IED Centre of Excellence (COE), Lieutenant Colonel Jose M Rufas provides a most enlightened and, at the same time, sombre assessment of the issue of fake explosives detection devices. The assessment is based on a detailed investigation undertaken by the COE. Counter-IED Report highlighted this very serious problem in its Autumn/Winter 2013 Edition. Snake oil salesmen around the globe have made and continue to make very large sums of money in the sale of worthless alleged detection devices. Rufas points out that in 2009 Iraq expended some $80 million on such devices. This was the result of high level corruption and criminality in both Iraq and the UK and resulted in custodial sentences in both countries.

In a perfect scientific and technological riposte to the fake explosives detection devices described by Lt Col Rufas above, Simon O.Williams, MD, Tactique Services, in his article explores the various types of technology on the market to provide procurement officers and operators with an overview of explosives detection solutions. He gives comprehensive descriptions of six Explosives Trace Detection solutions based on proven science and technology which are being manufactured and deployed commercially. These are in stark contrast to the bogus devices described in the preceding paragraph.

In his comprehensive article, John D. Howell of DSA Detection examines the issue of the density ranges of explosives for developing X-Ray detection windows for explosives at security checkpoints. He points out that there is inevitably pressure on security supervisors to speed up throughput in the checkpoint operation. For checkpoints using a cabinet X-Ray detection system, a key interest is the question of false detection alarms on mundane, non-threatening items. Automatic detection density windows can be adjusted to reduce the false alarm rate and thus increase checkpoint throughput. He, however, illustrates that extensive research and his own experience in this field leads him to conclude that narrowing explosives detection windows to reduce false alarm rates does not streamline an effective screening operation.

These and other excellent articles constitute this edition of Counter-IED Report. ■

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.

CHANGES IN THE COUNTER–IED OPERATIONAL ENVIRONMENT

By Russell McIntyre, former US Department of Defense

INTRODUCTION

We no longer face a unitary threat environment. The potential range of future Operational Environments (OE) will likely contain a more complex diverse range of potential threat capabilities and systems that will populate the battlespace. For over a decade the threat environment that faced the US and its Allies, coalition partners was relatively stable. There were two key theaters of operation, Iraq and Afghanistan; their primary weapon (principal casualty producer and cause of material damage) was a variety of improvised explosive devices. During that decade of counter-insurgency operations, due to the hard earned experience gained through recurring deployments returning to familiar terrain, there were few outright surprises but rather a grinding struggle for control of key geographic areas, keeping lines of communication open, suppressing insurgent activity/sectarian violence and the building of national institutions. Coalition Forces were the dominant battle space owners and essentially exercised sovereign control over the Counter-IED fight, defining the rules for its conduct, material and personnel exploitation and the disposition of information acquired. As the fighting was occurring in Iraq and Afghanistan, the national C-IED suite of capabilities expanded to include; more EOD force structure and technical capability, new organizations emerged like the Joint Improvised Explosive Device Defeat Organization (JIEDDO) with a significant budget, and the fielding of forensic laboratories to support theater operations. The hard earned lessons acquired that drove the growth of capability and shaped its operational contours need to be evaluated relative to potential theaters of operation and the threats therein that the US, its Allies, NATO and future coalition forces will likely face now and in the near-future.

A BLENDED THREAT ENVIRONMENT

In future operational environments US Forces and its Allies will face a range of capabilities that will include state sponsored provision to terrorist and insurgent groups of highly capable weapons systems that can challenge selected areas where they fielded superior capability. In an April 2015 article in Military Review, Lieutenant General, USA, McMaster outlined what constituted the threat picture US forces would face: "It is clear that Army leaders and units must be prepared to fight and win against state and non-state actors. Due to what some have called the democratization of destructive power. Non-state actors, such as the Islamic State of Iraq and Syria (ISIS) and Hezbollah possess capabilities previously associated only with the field forces of nation states."[1] A very recent example of state sponsorship is, according the Commander of US Navy Central Command (NAVCENT) Vice Admiral Kevin Donegan, that Iran provided coastal defense cruise missiles to *Houthi* rebels in Yemen which have targeted US warships engaged in interdiction operations off the coast. The Iranians are suspected of

providing training in the use radar systems to support the cruise missile attacks as well as the operation of the missiles themselves.[2] The EOD operator will not only be dealing with the improvised threat yet again but will also perform a more traditional task – the identification and reporting of first seen ordnance on the battlefield with the concomitant requirement to render it safe. An important role in direct support is the provision of warning to the Commander of new enemy threats on the battlefield. In a paper for the RAND Corporation military analyst David Johnson pointed to what he called the 'middle threat'. Occupying that space are the 'middle adversaries': "…middle adversaries are essentially state-sponsored hybrid forces characterized by capabilities on both ends of the spectrum. Thus they have the same set of weapons that irregular forces have but also additional capabilities, such as anti tank guided missiles (ATGMs) and Man-portable air defense weapons (MANPADs) and longer range, large caliber rockets."[3]

A LOOMING COLOSSUS - THE MEGACITY

The C-IED community will be faced by the numerous and new complex military geographic challenges that will include those posed by supporting operations in what is being called 'the megacity' environment, urban sprawls with populations of 10 million or more inhabitants with examples like Lagos, Nigeria or Cairo, Egypt. The aspects of this environment that heighten its challenge for the Commander include, but are not limited to, the following: "1) Extended urban infrastructures supporting dense, diverse populations, 2) Formal and informal sources of power, 3) Congested and constraining terrain, and 4) Interconnected, embedded threats across super-surface, surface, sub-surface, and cyber/space."[4] In The Army Chief of Staff's June 2014 Strategic Studies Group study on the Megacity environment the authors concluded that; "It is inevitable that at some point the United States Army will be asked to operate in a megacity and currently the Army is ill-prepared to do so."[5]

Specific facets of this operational environment that will directly impact Service EOD capability to support the Commander include: 1) A cluttered electromagnetic (EM) environment with public, governmental and commercial users who will insist on their access to the airwaves requiring very discreet jamming capability which requires building a detailed characterization of the various spectra in use, 2) A local populace and its governing bodies that will likely insist on minimal collateral damage as the result of IED neutralization, which could require increased use of manual entry and surgical device disruption, 3) EOD robot systems that have the tools and power to access a range of cars and commercial vehicles that would resemble the Wheelbarrow series developed by the UK to support C-IED operations in Northern Ireland, 4) Increased use of time as means to detonate devices placing increased pressure on EOD Teams to render safe devices with minimum collateral damage (use of time to control detonation of an IED was a tactic frequently employed by the Provisional Irish Republican Army bomb makers in Northern Ireland) and 5) A subterranean IED detection and neutralization capability for the sub- surface challenge posed by the enemy using tunnel systems to include those already in place for sewer, water, power lines, etc. to hide, conceal arms, explosives (as evidenced by Syrian rebels adopting a Medieval siege technique, undermining and collapsing stout Syrian Army field fortifications with improvised explosives) and move undetected beneath the surface. The maze of alleys, side streets and urban clutter found in cities also provides unique targeting opportunities for the use of VBIEDS. Although not a 'megacity' per se Mosul today is providing opportunity for ISIS to use their improvised armored VBIEDs in direct support of defensive efforts: "…the dense urban sprawl of Mosul, has created a nightmare scenario for Iraqi troops entering the city. Suicide vehicles spring from back alleys and cut in and out of side streets before striking Iraqi vehicles. The speed of the car bombers and an urban environment packed with civilians have made airstrikes against them almost impossible. Col. John Dorrian, spokesman for the USled campaign against the Islamic State, confirmed the problem, saying that the deeper into the city the Iraqis get, the harder it is for US air power to stop the suicide vehicles."[6]

THE ENEMY BELOW

The sub-surface challenge is not totally new to the US Army and Marine Corps as they both fielded ad-hoc teams, known as tunnel rats, to explore and then neutralize extensive Viet Cong and North Vietnamese sub-terrain networks. After the war in Vietnam the Tunnel Rat experience faded because it was regarded as a unique threat that would not likely appear in the future threat that the US Army envisioned post that conflict – facing the Warsaw Pact in Central Europe. This spatial dimension of the threat environment has unfortunately returned.

The sub-surface threat gained prominence during the 2014 Israel–Gaza conflict also known as Operation Protective Edge. Using experience gained in building smuggling tunnels from the Gaza Strip, under the border with Egypt (also known as the Philadelphi Corridor), the armed wing of HAMAS excavated over 35 tunnels from Gaza into Israel to avoid Israeli Defense Forces technical surveillance and border security forces. The tunnels were well constructed incorporating electric power, air circulation systems and mini-rail tracks to move excavated spoil and material. They were a surprise in both their scale, but also their highly efficient design incorporating the urban sprawl of Gaza City to help conceal the effort. The Israeli Defense Forces (IDF) were forced to improvise a counter-tunnel capability to include entry units, robotic reconnaissance and EOD systems. On 10 March 2015 the U.S. Congress passed the "United States-Israel Anti-Tunnel Defense Cooperation Act." The act states that "upon request of the Government of Israel and acting through the Secretary of Defense and the Secretary of State, it is authorized to carry out research, development, and test activities on a joint basis with Israel to establish an anti-tunneling defense system to detect, map, and destroy underground tunnels from Gaza to the territory of Israel or other countries that share a border with Gaza." [7] The act would appropriate 200 million dollars to support the joint US and Israeli research, development and test activities. This act should assist the Department of Defense, with their IDF partners gaining additional insight on how to counter this version of the threat. A simpler but still effective variation of the sub-service threat is being faced by Iraqi forces as these begin to clear out ISIS held areas.

The Iraqi Army has discovered that ISIS is making extensive use of tunnels to conceal movement, store supplies, and provide protected living areas for their fighters, incorporating this effort into their defense of urban areas. Drilling machinery normally used to support oil field operations, has been adapted by ISIS to efficiently establish networks of tunnels in rocky terrain that would be a difficult task using hand tools. Iraqi Commanders operating in the Mosul area '…knew urban warfare among civilians and human shields in Mosul would be difficult, but the tunnels are making it worse. The officers described the battlefield as more of a sphere than a plane – with threats coming from side to side above and below." [8] The Iraqi Special Forces and *Peshmerga* units are reporting that the tunnels-their entrances/exits - are frequently booby-trapped. Presenting yet another unique threat environment for EOD operators who will be needed to support the clearing, and exploitation of material found in the tunnels.

The US Military Services' operational experience in subterranean operations may have faded but current expertise in this area resides in the US Border Service. They have gained their expertise in the detecting, exploring and neutralizing Mexican Criminal Cartel tunnels built for moving large volumes of illicit drugs into the US. The Border Service has fielded special trained Tunnel Entry Teams to help map their path, evaluate their design and estimate the relative illicit drugs through put they could sustain. "Between 2006 and 2013, the average completed tunnel in the San Diego area had air vents and machinery to transport drugs. They also extended roughly 1,750 feet and were about 3? feet wide, according to statistics provided by US Immigration and Customs Enforcement officials." [9]

UNMANNED AERIAL SYSTEMS

In "Joint Operational Environment- 2035 The Joint Force in a Contested and Disordered World" the authors identified three emerging trends associated with the threat posed by "privatized violence"

(privatized violence incorporates sub-state, transnational criminal organizations and other irregular threats) incorporating Unmanned Aerial Systems (UAS) within their arsenals a threat weapons system.[10] These three trends are: 1) Adaptive irregular/sub-state adversaries – ISIS is an exemplar of this behavior, 2) Disruptive manufacturing technologies and the urban arsenal – 3D printing would fit in this category, and 3) The weaponization of commercial technologies – an armed UAS complimented by smartphone GPS and frequency hopping capability. The UAS which appeared as a hobbyist toy is emerging as a multi-functional terrorist tool capable of delivering explosive charges, conducting surveillance or interfering with aerial port operations: "…hobbyist drones are often less discussed within a security context, though they perhaps hold the greatest potential for achieving overmatch against the United States in the near term. Indeed, hobbyist drones are growing increasingly sophisticated – offering autonomous flight, high-end ISR capabilities, and ever-expanding payload capacity, range, and endurance. They are also widely accessible to potentially disruptive actors and, because drones assembled from component parts, generally do not have identifiable markings, could increase the difficulty of attribution if used in an attack. In addition, due to their size, construction material, and flight altitude, hobbyist drones are difficult to defend against if their presence in a particular area is unknown or unexpected." [11]

During the 2015 EOD Conference sponsored by the National Defense Industrial Association held in Bethesda, Maryland the Commander of the Naval Surface Warfare Center (NSWC) EOD Technology Division, Captain, USN, Vincent Martinez stated that; "I personally believe that the unmanned platform is going to be one of the most important weapons of our age."[12] Captain Martinez expressed concern that; "I'm going to have to start thinking not only about how I defuse the payload but how I defuse the platform. When I walk up on that platform, is it watching me, is it sensing me, is it waiting for me?"[13] This threat became very real when an Islamic State drone with an explosive main charge killed two Kurdish Peshmerga troops and seriously wounded two French paratroopers on the 2nd of October, 2016 in the vicinity of *Erbil*, Iraq.[14] The Counter-IED community, as early as 2014, has recognized the potential threat that the UAS present. This recognition is due largely to the experience gained by the C-IED community in countering the IED threat in Iraq and Afghanistan appreciating the capacity for insurgents and terrorists to adapt commercial technologies for a military purpose. The ability to recognize the threat potential of commercial technologies is relatively new and one where the C-IED community of operators and laboratories may hold an intuitive advantage over the intelligence communities' more established Technical Intelligence disciplinary areas that are focused more on weapon systems developed by Nation States.[15]

AN IED THREAT PICTURE

In a May 2016 article the Economist profiled the rise of improvised weapons beginning with the innovative designs of Syrian militant groups in what it called the "Hell's Kitchen of Aleppo".[16] This improvised threat fare has been a persistent threat in the Middle East and across the globe since gunpowder appeared. The lethality and effectiveness of improvised weapons is subject to being continually improved by complimentary commercial technologies that can dynamically enhance its; delivery, precision, and effectiveness. These innovative trends are being accelerated by their continuous use on the battlefield, evolving in effectiveness and inventiveness in their application. What is of particular concern is that the access to the battlespace by US, NATO and allied EOD operators and Technical Intelligence specialists that would allow timely identification of threat evolutions in capability, design and technological sophistication has significantly declined. Also it is very difficult to anticipate threat evolutions with confidence when the current baseline of enemy capability is not known. Currently access to events, areas of significant enemy activity is limited and when it does happen it is not timely, if it occurs at all. In the aforementioned circumstances it is very difficult, if not impossible, to establish and maintain a common IED threat picture. This circumstance is a far cry from when US and Coalition Forces had

the ability and authority to recover IED material from incident sites or from enemy caches, insert it into the expeditionary laboratory systems present in Iraq and Afghanistan for a quick turn assessment and back to national laboratories, as necessary, for a detailed technical assessment.

There is now a greater dependence on contribution of non-traditional partners who because of unique business and humanitarian relationships have access to the battlefield that government, departmental entities, the Services no longer have. An example is the work being conducted by the LLC and UK based Conflict Armament Research (CAR) in Iraq and Syria. A representative publication available published by CAR is "Tracing the Supply of Components used in Islamic State IEDs."[17] The reporting of commercial entities like CAR from combat zones where the C-IED community lacks direct or intermittent access will be of increased importance as the aperture of our IED activity window becomes increasingly limited.

What would improve our visibility on the improvised weapon development is a common threat picture which would serve as an authoritative source to guide training, countermeasure development and force protection initiatives. The Presidential Policy Directive for Countering Improvised Explosive Devices called for, as part of its plan to translate policy into action, to "… improve our understanding of technologies, trends and networks."[18] That understanding would occur through "Conducting multi-mode data analysis of IED patterns, trends, and tactics, techniques, and procedures to anticipate future IED threat evolutions."[19] All in name a description of a common IED threat picture that the C-IED community needs at different levels of classification to provide the analytic and technical baseline to measure their efforts against for sufficiency. Publication of an authoritative current IED threat picture would greatly assist in the collaboration among those responsible for countering it within the Department of Defense and – national/state/local law enforcement entities, our NATO partners, Coalition members and international law enforcement. Unfortunately PDD 17 did not specify just who was responsible for building and maintaining that common IED threat picture, relegating its production as an aspirational goal, the outline of a good idea, as opposed to a policy directing specific action by a department of government.

OBSERVATIONS

The future operational environment for the Counter-IED community is facing a period of greater uncertainty in terms of the threat and under what military geographic circumstance – will it be the Megacity described earlier in this article? What is compounding difficulties is that absence of an authoritative threat baseline tailored to major geographic regions to help guide training, equipment development and exercise design. Despite these vagaries it is not stopping, at least here in the United States, the reduction of EOD force structure built with such difficulty, cost and sacrifice. What logic is operating that is driving these reductions is not clear. What is needed is a systematic mission area analysis based on an authoritative threat estimate before more capability is shed. Further this analysis should be done in collaboration with our Allies and partner nations whom we will likely, yet again, be engaging a clever, determined and technologically savvy foe who resides at the end of that "Long Walk" our EOD operators will inevitably have to make. ■

REFERENCES

1 Lt. Gen. H.R. McMaster, Ph.D., U.S. Army, "Continuity and Change: The Army Operating Concept and Clear Thinking about Future War," *Military Review* 94, no.2 (2015): 16.

2 Courtney Kube, "U.S. Officials: Iran Supplying Weapons to Yemen's Houthi Rebels," NBC News, 27 October 2016, 4:54 PM ET: http://www.nbcnews.com/news/us-news/u-s-officials-iran-supplying-weapons-yemen-s-houthi-rebels-n674181

3 David Johnson, "The Challenges of the "Now" and Their Implications for the U.S. Army," RAND Corporation, accessed October 27, 2016: http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE184/RAND_PE184.pdf

4 Kevin M. Felix, Fredrick D. Wong, "Megacities: Pros and Cons – The Case for Megacities" Parameters, U.S. Army War College 4, no. 1 (2015): 24.

5 Colonel Marc Harris, USA, Lieutenant Colonel Robert Diao and Major Nicholas Melin, *"Megacities and the United States Army: Preparing for a Complex and Uncertain Future,"* (Washington, DC: United States Army Strategic Studies Group, 2014), 3.

6 Thomas Gibbons Neff, "ISIS video shows how the group has turned car bombs into its version of airstrikes," *The Washington Post*, November 15, 2016. https://www.washingtonpost.com/news/checkpoint/wp/2016/11/15/isis-video-shows-how-the-group-has-turned-car-bombs-into-its-version-of-airstrikes/?utm_campaign=Early%20Bird%20Brief%2011.16.2016&utm_medium=email&utm_source=Sailthru

7 United States-Israel Anti-Tunnel Defense Cooperation Act of 2015, 114th Congress (2015) URL https://www.congress.gov/bill/114th-congress/house-bill/1349/text

8 William Booth and Aaso Ameen Shwan, "ISIS Tunnels Complicate Fight for Control of Mosul," *The Washington Post,* November 6, 2016, sec. A.

9 Jason Song, "Claustrophobic? Don't even think of joining the Border Patrol's 'tunnel rats," Los Angeles Times May 3rd, 2016, http://www.defenseone.com/threats/2015/06/isis-using-tunnel-bombs-iraq/114730/

10 Joint Chiefs of Staff, Department of Defense, *Joint Operational Environment – 2035 The Joint Force in a Contested and Disordered World,* (Washington, DC, 2016),14 http://www.dtic.mil/doctrine/concepts/joe/joe_2035_july16.pdf

11 Kelly Sayer, *A World of Proliferated Drones: A Technology Primer* (Washington, DC: Center for New American Security, 2015), 29, http://drones.cnas.org/wp-content/uploads/2016/03/CNAS-World-of-Drones_052115.pdf

12 Joe Gould, "US Military's Bomb Techs Fear Flying IEDs," *DEFENSE NEWs*, July 28, 2015. http://www.defensenews.com/story/defense/policy-budget/warfare/2015/07/28/us-militarys-bomb-techs-fear-flying-ieds/30747275/

13 Ibid.

14 John Irish, Jean-Baptiste Vey and Marine Pennetier, "Islamic State drone kills two Kurdish fighters, wounds two French soldiers," *Reuters*, October 12, 2016. http://www.reuters.com/article/us-france-iraq-iraq-idUSKCN12B2QI?il=0

15 NOTE: For an excellent and very recent analysis of the UAS threat posed by terrorists please refer to the Combating Terrorism Center at West Point's study "Remotely Piloted Aviation: Terrorism, Drones and Supporting Technology," by Don Rassler, October 2016. https://www.ctc.usma.edu/v2/wp-content/uploads/2016/10/Drones-Report.pdf

16 "Hell's Kitchens: Makeshift weapons are becoming more dangerous with highly sophisticated, commercially available kit," *The Economist*, May 21 2016, 69-70.

17 "Tracing the Supply of Components Used in Islamic State IEDs: Evidence from a 20-month investigation In Iraq and Syria," Conflict Armament Research Ltd. Web, last modified February, 2016. URL http://www.conflictarm.com/wp-content/uploads/2016/02/Tracing_The_Supply_of_Components_Used_in_Islamic_State_IEDs.pdf

18 Presidential Policy on Countering Improvised Explosive Devices (PPD 17), U.S. White House, 26 February 26, 2013. 2. Accessed November 10, 2016. https://www.whitehouse.gov/sites/default/files/dos/cied_1.pdf.

19 Ibid.

ABOUT THE AUTHOR

Russell McIntyre competed a 46 year career in the Department of Defense (DOD) as a serving officer in the US Army that included duty in South Vietnam and Iraq and in 1997, returning as a Civil Servant with duties that included supporting the Counter-IED fight in Iraq, with an assignment in 2004 to the MNC-I Counter-IED Cell, and later fielding Forensic Laboratory capability in Iraq and Afghanistan.

C-IED EDUCATION AND TRAINING – THE WAY FORWARD

By Torsten Gottlieb, Lieutenant Colonel DEU Army, Branch Chief
Philippe Belda, Lieutenant Colonel FRA Army, Lessons Learned Section Chief
Jose Lopez Navarro, Lieutenant Commander ESP Navy, Training Section Chief
Dragos Gheorghe, Major ROU Army, R&D Analyst within LL section
Niklas Tornesjo, Lieutenant Colonel SWE Army, Exercise Coordinator Training Section
Levente TÁBI, Lieutenant Colonel, Hungarian Army / Engineer Corps

INTRODUCTION OF THE COE

In September 2007, the Spanish Minister of Defence announced his decision to put on offer a Counter Improvised Explosive Devices Centre of Excellence (C-IED COE), to serve as an international touchstone in the counter terrorism struggle.

The main intention was not only to contribute to the overall well-being of the troops and civilians involved in, but also to the security of the allies.

Towards the end of 2007, the Spanish Chief of Defence, through the Allied Command Transformation, formally offered to NATO a multinational Counter-IED COE. In 2008, the Transformation Command confirmed that the future COE concept fully met with Allied principles.

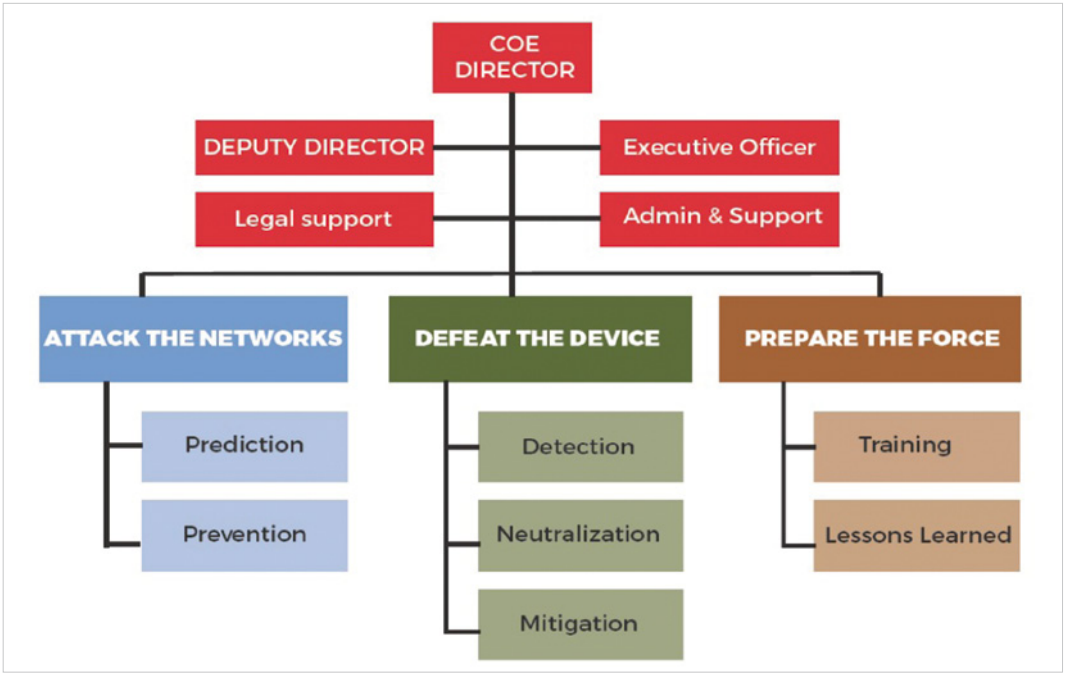
Prior to joining the NATO COE community, ACT had to certify that the facilities, quality and level of readiness offered to the allies matched the NATO standards. In June 2010, six countries signed the Memorandum of Understanding in Norfolk, Virginia.

The Centre of Excellence is one of the primary actors mentioned in the NAC approved C-IED Action Plan, which is “aimed to reduce the strategic impact of IEDs in Afghanistan and future conflicts by limiting their tactical and operational effects”. It identifies actions required to be fulfilled by the NATO and C-IED COE from 2010 onwards.

IEDs are nothing new. They have existed for hundreds of years and have been used all over the world. In the recent conflicts in Afghanistan and Iraq the use of the IED emerged as the single most effective enemy weapon. The IED is a weapon that threatens the safety and security not only of partner nation combatants, but the welfare of the general population within the area of conflict. The IED is a faceless weapon that can have significant strategic, political, operational and tactical effects.

Threat networks use IEDs because they are cheap, easy to build, composed of readily available dual use components and are effective. The current device technology is usually low-tech often utilizing command wire or simple victim operated initiation systems and the explosives used typically are military munitions, explosive remnants of war (ERW) or home made explosives (HME). The current threat networks continue to build capability and capacity through the internet and social media to rapidly disseminate IED technology, tactics as well as extremists ideology.

These facts along with global instability and the potential strategic effects of the IED will result in the use of the IED as a weapon of our adversaries in future conventional, Irregular and Hybrid conflicts.



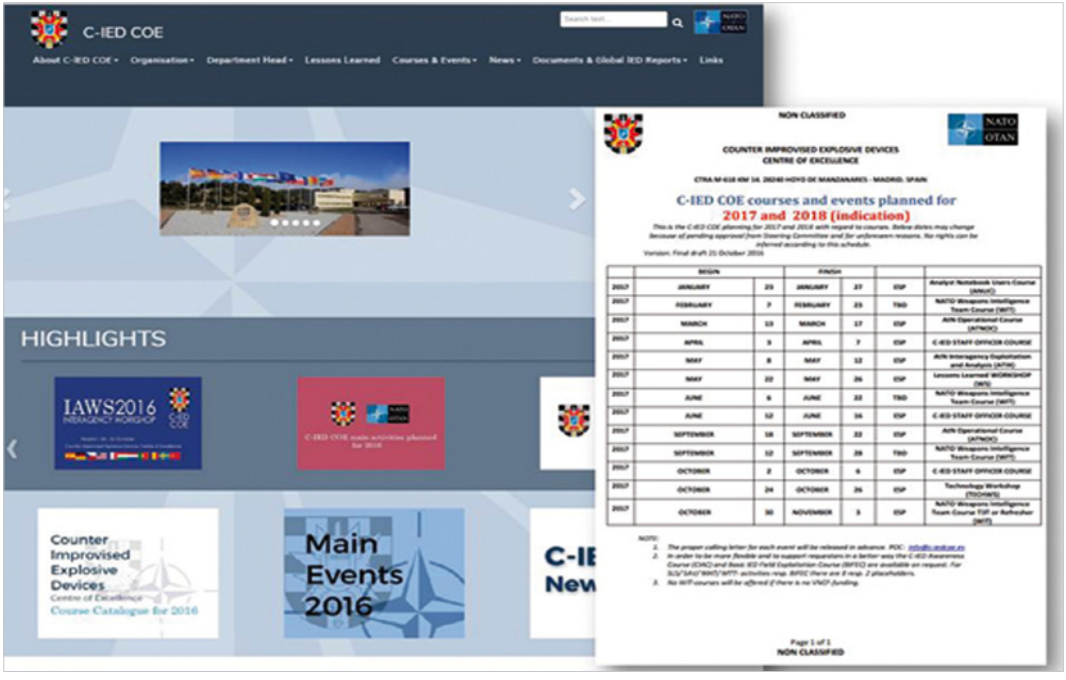
The C-IED COE aims to counter this threat by becoming the pre-eminent source of innovative expertise on all multinational aspects of C-IED in support of our sponsoring nations. By becoming NATO's C-IED transformation expert and the focal point for C-IED education and training for NATO and other Allies we will reduce the operational impact of IEDs within our nations and on the battlefield.

DEPARTMENT HEAD (OF TRAINING)

NATO HQ Supreme Allied Command Transformation (SACT) is responsible for the overall management of NATO Education and Training (E&T), and this is achieved through a governance structure. Within this governance structure a Requirements Authority (RA) and a Department Head (DH) are appointed for each discipline. The RA and the DH support the centralized coordination and decentralized execution of NATO E&T activities and events. The C-IED COE is the Department Head for the C-IED discipline within NATO.

E&T is just one potential solution for eliminating the multitude of causes of a performance gap, a difference between actual and desired performance. If a performance gap can be translated into an E&T gap, the competent RA has to identify it as a NATO E&T requirement. The DH will check the requirement against the available E&T opportunities and coordinate an appropriate solution. The C-IED COE coordinates E&T solutions with the E&T Solution Providers. The **new** webpage of the C-IED COE (http://www.ciedcoe.org) provides an overview about courses the COE will conduct in 2017.

The Defense Against Terrorism (DAT) COE, the C-IED in the Maritime Environment with the NATO Maritime Interdiction Operational Training Centre (NMIOTC), the Explosive Ordnance Disposal COE (EOD COE) or the Military Engineering Centre of Excellence (MILENG COE) and in the future the Human Intelligence COE (HUMINT COE) are institutions with which the C-IED COE has a permanent contact to coordinate C-IED in those disciplines.



Annually the C-IED COE acting as DH is responsible to organize the Annual Discipline Conference (ADC) where all the stakeholders of the discipline meet to review NATO E&T requirements related to C-IED and verify the adequacy of the discipline-specific E&T programme to satisfy the requirements. The intent is to ensure E&T remains aligned with evolving needs and to determine the way ahead in closing gaps while further developing the discipline.

Further information about the NATO E&T Systems Approach to Training, DH-related documents and activities in the C-IED discipline, course documents and calling letters to all of C-IED COE courses are available via Transnet, ACT's Internet portal within the "support to C-IED"-page (https://ete.transnet.act.nato.int/CounterImprovised%20Explosive%20Devices/Forms/AllItems.aspx)

QUALITY ASSURANCE

Since 2016 C-IED COE is accredited by NATO as a training institution, providing orientation, defining procedures and methods for CIED COE efforts to follow up, support and develop the education in the C-IED discipline.

The purpose of Quality Assurance (QA) is to provide confirmation to the Alliance that courses conducted in the C-IED COE meet NATO E&IT Requirements, and are delivered utilizing an effective Quality Management System (QMS).

Because NATO certified courses delivered by the C-IED COE met NATO E&IT requirements and the COE is an institution accredited by it, all courses conducted in the C-IED COE are categorized as NATO APPROVED courses.

COURSES

As the NATO Department Head for C-IED, the C-IED COE fills an important role to support the institutionalization of C-IED within NATO, which includes the whole process from individual training and courses to collective training and exercises. The C-IED COE new landscape of courses focusing on the joint operational level is directly related to NATO's

C-IED capability and the observations, lessons identified and the validation results from these exercises. This evolution of courses, especially the C-IED Staff Officers Course (CSOC) and the Attack the Network Operational Course (AtNOC), but also the Attack the Network Interagency and Exploitation Course (ATIX) have been developed and calibrated in order to support NATO to fill these identified gaps.

Also, the C-IED COE conducts a Tactical level course to train Nations in Level 1 exploitation, the Weapons Intelligence Team Course (WIT).

The CSOC course aims to provide C-IED Staff Officers and Senior Staff Assistants, at upper tactical (e.g. in the Land Component Commands [LCC]) and operational levels, with the knowledge and skills to facilitate, manage and lead the C-IED effort, by drawing together and coordinating the expertise and efforts of the other staff branches, and become the Commanders' primary C-IED SME and operations advisor.

AtNOC aims to provide J2, J3, J5 and C-IED Staff Officers and Senior Staff Assistants, at upper tactical and operational level commands the knowledge and skills to facilitate, manage and lead the AtN effort, by integrating the supporting C-IED/AtN programs with intelligence, operations, planning and targeting within the HQ. Emphasis will lay on intelligence and targeting processes.

ATIX aims to provide the students with the basically (technical and) tactical understanding of exploitation products and processes. These include Biometrics, Forensics and DOMEX products produced during IED laboratory exploitation, and how they support operational level multi-national military operations.

The WIT-course aims to provide essential Level 1 Exploitation Weapons Technical Intelligence (tactical level) training to teams in order to respond to IED incidents – prior to their arrival in an Operational Theatre. Weapons Intelligence Teams will be trained to investigate IED incidents and produce s tandardized tactical, technical and forensic

intelligence Level 1 reports that can feed the Operations and Intelligence cycle to more effectively understand and conduct Attack the Networks activities (e.g. such as Targeting, Evidence Based Operations, Law Enforcement and/or Influence operations.

For 2017 the C-IED COE has planned three iterations for the CSOC, two for the ATNOC, one ATIX and four WIT courses.

Next to the classified courses for NATO countries and partners, C-IED COE developed the Basic Field Exploitation Course (BIFEC) and C-IED Awareness Course (CIAC) as unclassified versions for new partners of NATO.

For all of these courses the C-IED COE developed during the last two years pre-requisite Advanced Distance Learner courses (ADL) with support of ACT Joint Force Trainer (JFT). Currently every potential student of CSOC, AtNOC and WIT received four or eight weeks prior to the residential phase of the course his access to the ADL course in order to learn, repeat and fulfil minimum requirements as further course student. Next to the three courses related ADL for CSOC, AtNOC and WIT the C-IED COE developed a generic awareness ADL course, available for everyone inside NATO. (Contact for your own login: https://jadl.act.nato.int)

EXERCISES

With focus on enhance NATO HQs C-IED capability and particularly their “Attack the Network” capability against an IED-system, the C-IED COE frequently supports NATO’s joint operational command post exercises, even known as the Trident-series.

The C-IED COE aim with the exercise support is to boost the institutionalization of a de-compartmentalized C-IED mindset within NATO HQs and fill the identified C-IED gaps on the joint operational level within NATO. The C-IED COE support to the Trident-series exercises have successfully resulted in that C-IED and Counter Threat Network activities have been comprehensively and cross-functionally implemented in these exercises. Our

intent is to encourage NATO HQ's to conduct the full spectrum of C-IED activities on the joint operational level (in line with NATO doctrine) and increases their capability to counter network or adversaries utilizing IEDs.

The exercise support provides the opportunity to evaluate the HQs' C-IED capability and directly influence a broad audience within NATO HQs, including senior leaders and increase the understanding of C-IED as a comprehensive and cross-functional effort that shouldn't be compartmentalized or stove-piped.

However, the exercise support is only one part of C-IED COE commitment. The identified criteria for success, is when C-IED is comprehensively and cross-functionally implemented within the HQs' working groups, coordination boards and the different branches' current staff processes. These traditional Staff activities receive and integrate the C-IED cells particular technical expertise, rather than rely on the staff C-IED cell to carry-on a separate, parallel staff process.

LESSONS LEARNED

Strategic Command SACT (Supreme Allied Command Transformation) and SHAPE (Supreme Headquarters Allied Powers Europe) initiated the establishment of the NATO C-IED Community of Interest (CoI) on the NATO Lessons Learned Portal (NLLP) nominating the C-IED COE as the "content manager" for the CoI in support of the COE task as the "NATO out of theatre C-IED Lessons Learned coordinator". The C-IED COI-portals are now established on NLLP (both in the unclassified and the classified domains) after cooperation and with support from the JALLC. The main objective is to share, collect and disseminate C-IED related observations, Lessons Identified, Lessons Learned, knowledge, reports and other C-IED lessons and documents in theatre as out of theatre, being a one stop shop. The registration must be done in JALLC portal: https://nllp.jallc.nato.int/Pages/default.aspx

Send an email to the LL portal managers (jcurras@ciedcoe.org / pbelda@ciedcoe.org and pbelda@esp.bices.org) with your user name and state that you applying to get access to the C-IED CoI portal.

A C-IED CoI user could have access to these documentations and upload any document for the benefit of the community.

All new TTPs analysis and LL could eventually be incorporated in our courses/training.

The Lessons Learned section conducts an annual LL Work Shop. The 5th Counter Improvised Explosive Devices (C-IED) Lessons Learned Workshop (LLWS) was held in December 2015 at the C-IED COE. This 2015 workshop emphasized the C-IED Defense Capability Building (DCB) and Security Forces Assistance (SFA) processes within NATO and other international organizations such as the UN and others. It was an opportunity to share information regarding C-IED DCB and to develop possible solutions and recommendations for C-IED DCB.

The next LLWS will be held 23-25 May 2017. ■

ABOUT THE AUTHORS

LTC Torsten GOTTLIEB (German Army / Engineer corps), graduated from the German "Helmut-Schmidt-University" of the Federal Armed Forces in 1999. Currently posted in the C-IED COE as Prepare the Force Branch Chief he started his career in the National People's Army (former GDR) 1986. He was appointed to Infantry and after German Reunification he joined the Engineer Corps of the Federal Armed Forces 1993. After his graduation from the university he fulfilled several roles and posts within military hierarchy as platoon leader, company reconnaissance officer, company commander, staff officer within Joint Support COM, Joint Medical COM and during his last assignment starting 2012 in the national C-IED Centre of the Joint Forces Operations COM. Starting with 2015, he was commissioned as Branch Chief Prepare the Force (PTF) of the C-IED COE. His operational assignments include Operational positions at the tactical and joint operational level in the Former Republic of Macedonia and several times in Afghanistan.

LTC Philippe BELDA (French Army / Engineer corps) graduated with a University Technical Diploma of civil engineering from Bordeaux and joined the Army in 1992. He joined the regular army from the reserve in 1996 and served from 2000 to 2006 in a combat engineer regiment as platoon leader and as a captain in command of a combat Coy. Following this he served at the French Army engineer school as an instructor for lieutenants and captains for 4 years. In 2010 he moved to the Force Headquarter n°3 (Etat Major de Force 3) working as a staff officer at the OPS division/ Plan office. Since 03/08/2015 he is posted to the C-IED COE as a Lessons Learned section chief. He has been a LTC since 01/06/2016. He is qualified as an EOD/ C-IED/military Search staff officer. His last overseas operations as a staff officer were in a HQ Planning staff in Ivory Coast (ONUCI) 2010, ISAF C-IED chief training in Afghanistan (Kabul, Bagram within US TF Paladin) in 2012 and J3/5 staff officer French HQ in Mali 2014. Next to these deployments he has had experience as a Coy Comd in Lebanon (2006) and as a platoon leader in Kosovo (2001).

Lt Cdr Jose LOPEZ NAVARRO (Spanish Navy / submarine corps), graduated from the Spanish Naval Academy in 1996. Currently posted in the C-IED COE as Training Section Chief. Vast majority of his career has been in Submarines as a Department Head of Engineering. In addition to his Submarine education, he attended other military courses regarding Education in the Spanish Armed Forces and in NATO, Education Auditor, Naval Engineering. Among his assignments, three years as a teacher in the Naval Academy, Manager in the Submarine Safety Program for the construction of a new Submarine in Spain, Executive Officer in a Frigate and Commander of a fast patrol boat.

Major Dragos GHEORGHE (Romanian Army / EOD corps) graduated from the Romanian Land Forces Academy in 1999 as an infantry officer. He was appointed in infantry and mountain troop units, fulfilling different roles within military hierarchy as platoon leader, company executive officer, intel staff officer, company commander, chief of current operations at battalion level, staff officer within General Joint Staff. Starting with 2012 he passed through several training courses in EOD and C-IED domains, becoming a senior instructor within Romanian EOD Training Base. Starting with 2015, he was commissioned as R&D Analyst within LL section / Prepare the Force (PTF) Branch of the C-IED COE. His operational assignments include Iraq, Afghanistan and during his current assignment in Madrid in a training mission in Amman (Kingdom of Jordan).

LTC Niklas TORNESJO, graduated from the Swedish Naval Warfare University in 1999 as a Costal Commando officer within the Swedish Amphibious forces. Currently posted in the C-IED COE in Prepare the Force Branch he started his career in the Swedish Amphibious forces in 1996 and he moved in 2003 to the Swedish Ranger Forces. After his graduation from the university he fulfilled several roles and posts within military hierarchy as platoon leader, company commander and staff officer within the operational and intelligence community, he has also been assigned to the Swedish Land Warfare Centre where he was responsible for the Ranger education and for the development of the Swedish Land forces C-IED capability. He has been involved in the development of the Swedish Armed Forces C-IED capability since 2008 and his operational assignments include Operational and C-IED positions at the tactical and joint operational level.

LTC Levente TÁBI (Hungarian Army / Engineer Corps) – graduated from the Kossuth Lajos Military College (A) Szentendre, Hungary in 1992. He was commissioned as Military Engineer and his assignments were from MILENG platoon leader up to the senior MILENG desk officer (MILENG advisor) at Hungarian Defence Forces Joint Force Command. Beside his MILENG education and experiences, he graduated as Civilian Engineer Teacher and in 2006 he attended the Hungarian Military Academy. His operational assignments include Afghanistan, 2007. He is currently the MILENG analyst in NATO C-IED COE, PtF Branch, Training Section.

THE ISLAMIC STATE IN IRAQ AND SYRIA IED REVOLUTION

By Greg Robin - Sahan C-IED Expert, Camille Chautard - Sahan Analyst and Stephanie Braquehais, Editor

The Islamic State in Iraq and Syria's (ISIS) massive industrial production and use of IEDs have revolutionised how a terrorist group can wage war. ISIS maintains control of territories they conquer by meticulously locking down the occupied areas with unprecedented numbers of Improvised Explosive Devices (IEDs). Its main objective is to create as many casualties as possible, military or civilian.

For the last twenty months, the Kurdistan Region Security Council (KRSC) granted access and support to Sahan's research on IEDs utilized by ISIS on the frontlines and in nearby towns. Sahan investigated different types of IED attacks, techniques, tactics and procedures employed by ISIS.

A SEMI-INDUSTRIAL PRODUCTION

With its standardised components, advanced procurement, logistical chains, systematic assembly and quality control mechanisms, ISIS IED production is executed on a very large scale and covers the spectrum of IED-making, from the artisanal to the industrial. The group has transformed what was once the "Improvised Explosive Device" into the "Industrialised Explosive Device". In ISIS controlled territories, the manufacturing infrastructure, from small workshops to large factories, is re-organised to produce IEDs, other munitions, and weapon systems. This semi-industrial process, no longer improvised, has led Sahan to rename IEDs as Unconventional Ammunition Explosive Devices (UAEDs).

The ability to resource, plan, and organise this production demonstrates a level of knowledge, experience, and willingness to deploy vast efforts that are unprecedented for a non-state actor. This is possible because ISIS controls large territories, an array of factories and a qualified workforce. There is also evidence that ISIS trains many of its fighters in basic IED-making. Sahan has come across a manuscript bomb-making manual as well as hand-written notes discovered by the Peshmerga EOD specialists in the Mosul Dam area.

These documents suggest that ISIS also trains its militants to assemble their own IEDs in the field when necessary, demonstrating the group's capacity to adapt its carefully planned and centralised approach to local circumstances.

This systematic transfer of knowledge covering a wide range of IED options requires a level of control and command and a flexibility that are uncommon for a terrorist organisation, enabling ISIS to use IEDs in all combat operations.

ISIS OPERATING METHODS

The most widely known use of IEDs by the Islamic State is for offensive purposes, specifically by conducting suicide attacks against its opponents. ISIS currently have three main methods to conduct suicide attacks: the suicide vehicle-borne IEDs (SVBIEDs), person-borne IEDs (PBIEDs), and Inghimasi/infiltrated fighters who are combatants who explode their suicide vests

Victim-Operated Directional Fragmentation Charge (VODFC) with scale reference (photo previously published in FT).
Photo Credit: Sahan.

Since 2014, the Islamic State has considerably developed the use of IEDs for defensive purposes. Indeed, most IEDs observed in Iraq and Syria by Sahan during the last 20 months are victim-operated IEDs (VOIEDs) used for area-denial.

Although the most common types of VOIEDs (victim-operated IEDs) are pressure plates and crush bead pressure switches, one new type of defensive VOIED resembling conventional Italian anti-personnel mines is widely used by ISIS for its defensive lines. Moulded in industrial-like plastic, it illustrates yet another level of manufacturing skill by ISIS. Built with a shaped charge, it is a victim-operated directional fragmentation charge (VODFC). This model has already been observed elsewhere in Iraq, in Shirqat and Qayyarah, suggesting a centralised production. Yet it is the first time that it has been observed laid out in long defensive lines across farmlands.

only as a last resort should they be wounded, captured, or about to be killed. Suicide attacks, especially conducted with SVBIEDs may be combined with several weapon systems and are often coordinated to attack several targets simultaneously.

At the Mosul offensive, coalition forces have already been faced with dozens of SVBIEDs on each front, sometimes several in a few hours, although coalition air and ground missile systems typically destroy them before they reach their targets. Now that the Iraqi army and the Iraqi Kurdistan Peshmerga have reached the urban areas of Mosul's eastern suburbs the campaign is getting more complicated. Militants are barricaded in buildings rigged with IEDs, using the civilian population as shields, and are deploying PBIEDs and snipers to erode their opponents' forces. ISIS sends relentless waves of suicide infantry at the Iraqi forces, preventing them from recuperating.

Pile of pressures-plates made in series by ISIS - Gwer, Kurdistan - October 2016.

Lines of victim-operated directional fragmentation charge (VODFCs) - Gwer Bridge, Kurdistan - October 2016.

PLASTIC AND METAL PLATES

The VODFC consists of an unconventional landmine made out of plastic and equipped with a metal plate. The explosive charge is made of an aluminium-based homemade explosive (HME). It is hidden under the surface of the ground, like a mine.

When pressure is put on the DFC (directional fragmentation charge) by a vehicle or individual, the explosive is activated, and the metal plate is propelled with the intent to damage or destroy armoured vehicles and/or kill or wound individuals. The detonation creates high pressure that propels the metal plate while simultaneously reshaping it into a single high velocity penetrator (shaped charge).

The high quality of the plastic container and the mechanism of the DFC, especially its firing system, show a high level of technical knowledge and manufacturing capacity. The plastic parts of the container suggest an industrial quality, while the stainless-steel pressure-plate and the fitting of the fuze and the detonator (with silicone and bolts) are handcrafted.

The ISIS DFCs are produced in series and in large scale, and are widespread at the Mosul front line on a band of at least 100 km. This new type of homemade mine used by ISIS could have been produced in a plastic factory located in occupied areas. The recent discovery of unfinished DFC components suggests that the victim-operated devices were assembled, if not produced, near Qayyarah.

Such a device represents a specific danger due to its material specifications. It will remain active and operational for a longer period of time in comparison with a pressure plate system exposed to weather conditions and having the limitations of a battery charge. Although the Sahan team documented at least three other similar VO devices equipped with identical pressure fuzes, this specific DFC is the most advanced ISIS VO device observed in Iraq.

IEDs collected by Peshmerga Combat Engineer Forces - Sinjar, Kurdistan - December 2015.

CHEMICALS AND DRONES

Another defensive tactic used by ISIS are command-wire IEDs (CWIEDs). As its name suggests, CWIEDs are detonated by individuals: a militant triggers the explosion at the right time, presumably when opposition forces enter the blast radius of the IED. CWIEDs are usually hidden at critical locations such as vulnerable points or unavoidable points of passage, and are typically used in urban and semi-urban areas for defensive purposes. They have also been used for withdrawal tactics.

Finally, ISIS is also experimenting with new unconventional weapon systems, such as chemical projectiles and weaponised drones. The proliferation of creative drone-borne IEDs (DBIEDs) made by ISIS in Iraq and Syria suggests the presence of a centralised production and skilled drone-makers eager to try out new tactics.

THE IED DECONTAMINATION PROCESS

IED clearance is a slow, dangerous, and highly specialised activity. For each metre of recovered territory, keen observation above ground level, along roads, and potentially of every inch of a building for the possible indicators that could help locate an IED is imperative. For instance, a difference in soil colour or texture, or a protruding wire or piece of IED that has not been well concealed could give clues to the presence of danger. When a suspicious sign is confirmed, the person conducting the search marks the spot. An explosive ordnance disposal (EOD) technician must then enter the danger zone and proceed to the identification of the IED in order to understand its mechanism. It should be conducted in a meticulous manner, with protective and detection equipment. The technician's progress is inevitably slow.

Yet, despite the Peshmerga EOD teams' excellent training, clearance works, and good knowledge of ISIS' IED techniques and tactics, the Kurdish EOD specialists are simply too few, and lack the required equipment. There are only a few EOD technicians in Kurdistan, and most of them are currently at the front helping their colleagues breach ISIS' defence lines. They are also in the newly liberated areas, marking which areas are safe or not and potentially saving civilians. They are not equipped with essential personal protective equipment that could save their lives, the technicians have very few jammers and

Sahan Map - Northern Iraq.

guided robots that could enter the danger zone in their place. The EOD technicians' attrition rate could be significantly reduced should they be provided with basic equipment.

MARKINGS OF DANGER AREAS

In the liberated territories, the first part of the decontamination process is concluding if an area is safe or not. This process has barely been initiated. This procedure, unless done in a systematic manner, becomes counterproductive and may pose further risk to returnees.

Although some markings of suspected hazardous areas (SHA), like graffiti, or in the best cases mine-signs painted in red, may be present in some areas, they cannot be considered reliable. They mark the known SHAs, but many contaminated areas remain unmarked. For example, in Sinjar, IED contaminated zones have been partially marked because of a lack of funds, and other pressing urgent needs. This situation arguably poses a bigger threat to civilians, giving the wrong impression that unmarked areas could be safe. Yet the absence of marking often simply implies that no comprehensive decontamination work has been done in that area. For instance, in Gwer, many contaminated areas remain unmarked. The task is simply too important for so few technicians, who are also needed at the front lines: they concentrate on the most immediate threat, such as clearing the main axes for their troops to pass before moving on.

THE NEED TO RECOGNISE IED AS A WEAPON

In sum, there is no systematic procedure to ensure that the decontamination process is efficient and safe. Although there is a national capacity to coordinate the demining, Iraqi Kurdistan Mine Action Authority (IKMAA) and a large number of private Kurdish technicians ready to work if required, there are currently no (or few) donors to fund such projects. This limited funding is largely due to the lack of international recognition of IEDs as an anti-personnel weapon. Although the Ottawa Convention bans the use of

conventional anti-personnel mines, IEDs are currently not considered due to their "improvised" nature even though they represent the biggest threat of our time. The semi-conventional use and semi-industrial production of IEDs on unprecedented scales by ISIS suggest that the legal framework is becoming obsolete. The Convention on Certain Conventional Weapons (CCW), and in particular its Protocol II on Prohibitions or Restrictions on the Use of Mines, Booby Traps and Other Devices, is the only instrument of International Humanitarian Law that explicitly mentions IEDs.

International law needs to recognise IEDs as what they are: specialised, mass produced weapons that indiscriminately target civilians. Before then, it will be difficult to mobilise the required funds for an activity that is not clearly defined by international law.

In this context, education programmes to help communities and humanitarian workers understand the risks associated with an IED threat never encountered at this level until ISIS, are key. Civilians who return to their homeland once liberated, cannot resume their livelihoods because their farming/grazing lands are swarming with IEDs, preventing the already weak economy from recovering.

MIGRATING THREAT

The IED threat in Iraq and Syria is unprecedented. Despite no reliable estimates, Sahan's field investigations suggest that the IED threat keeps growing. ISIS placed 3000 IEDs in Palmyra and several thousand in Baiji, Tikrit, yet the Peshmerga claim they have cleared more than one thousand IEDs at the Mosul front in only four weeks, without even having entered the city. The number of VBIEDs in today's Mosul campaign is unparalleled.

Despite today's efforts by the coalition to destroy the Islamic State, the IED threat is migrating towards other modes of operation, sometimes directly threatening Europe and North America, but increasingly spreading to other regions. In addition to training its own fighters in Iraq and Syria with IED-making, ISIS shares its IED skills and knowledge to its affiliates around the world. In Libya, the use of crush bead pressure switches - also known as crush wires - has widely spread since online forums provided instructions on how to build them. Similarly, the use of DBIEDs has spread from Syria to Iraq, and is expected to expand even further. The International community should expect that other groups, such as Boko Haram in Nigeria and Al-Shabaab in Somalia, will try to replicate the ISIS business model of an industrialised mass production of IEDs, depending on their control of the territory, the quality of local infrastructure (workshops, factories), local labour, and their financial resources.

Such knowledge is also reaching individuals who sympathise with the group's global aims. A new video released in November 2016 by ISIS gives simple instructions on how to make IEDs at home, urging ISIS sympathisers to build and use them where they live, especially in Europe and North America. Although this is a far cry from the large-scale industrialised process described above, security agencies are becoming increasingly worried at the prospect of witnessing IEDs proliferate within their own territories. ■

ABOUT SAHAN RESEARCH

Sahan Research is a think-tank dedicated to the promotion of peace, security and development through research, analysis and learning.

Its primary areas of focus are the Horn of Africa and the Middle East, where its core team possesses decades of experience in diverse fields, including:

- Regional political and security dynamics
- Governance in transitional and post-conflict environments
- Conflict prevention, mitigation and resolution
- Political facilitation and peacebuilding
- Risk management and security advice
- Monitoring and verification.

FAKE BOMB SEARCHERS: EXPLOSIVE DETECTION SCAM IS SCARING THE C-IED MARKET!

By Lieutenant Colonel Jose M Rufas, Head of the Defeat the Device Branch,
C-IED Centre of Excellence

"Lies can't sell without an atom of truth."
(Aniekee Tochukwu Ezekiel, in the book "Psychology of Friendship for Leadership", published in 2010)

This article is based on the outstanding investigation conducted by Jose Yenes & Denis Zöhner, which results could be read in a C-IED CoE report available through http://www.ciedcoe.org/news/2016/

After a deadly suicide improvised explosive device killed about 300 people in Baghdad, it was July 4th 2016, when Iraqi Prime Minister Haider al-Abadi banned the use of an already evidenced fake explosive detector called "ADE 651" (Advanced Detection Equipment 651); that decision came more than two years after he first acknowledged they were fake and promised to remove them.

Just after the bombing, the Ministry of Interior's website was hacked and a picture of a bloodied baby was posted along with a bomb detector bearing the Islamic State's markings. "I don't know how you sleep at night," the hacked site read. "Your conscience is dead." The fake detectors were publicly identified by the Iraqis as a symbol of government corruption and the state's failure to protect them.

In 2013 the owner of the company selling those detectors to Iraq was jailed for 10 years. Another person was convicted for seven years, due to his selling of more than 1,000 useless detectors (named as "GT200", they were home-made plastic boxes with handles and antennae) which he claimed could track down explosives, narcotics, tobacco, ivory and even cash, while he had claimed the GT200 worked with a range of 700 metres at ground level and as far as four kilometres in the air. According to public investigators and British prosecutors, the ADE 651 and similar fake devices had been sold to the Lebanese army, to the Mexican army, to the police in Belgium, and to the Mövenpick Hotel Group's property in Bahrain. It was also sold in Romania, Bulgaria, and the Republic of Georgia. In Asia, there were clients in Bangladesh, China, Hong Kong, India, Japan, Pakistan, Thailand, Afghanistan, Philippines, and Vietnam. In the Middle East, the device made it to Jordan, Qatar, Saudi Arabia, Syria, the United Arab Emirates, and Iran. In Africa, it was bought by Kenya, Libya, Niger, Djibuti, and Tunisia… But no country bought that equipment in the way Iraq did in 2009, expending more than 80 million dollars.

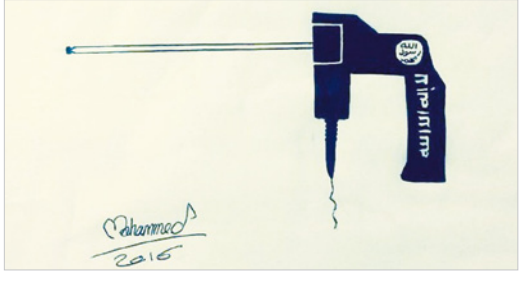


Figure 1: Hacked Iraq MOI website - partial image.
(Source: http://alrassid.org/news.php?NewsID=7731)

Figure 2: "GOPHER" golf ball finder.
(Source: http://www.bbc.com/news/uk-29459896)

EVERY TALE HAS ITS ORIGIN INSIDE A DREAM; HOW THE FRAUD DID START!

In the early 90s in the United States of America, an ingenious person started selling a device called "**GOPHER**", allegedly designed to find lost golf balls just using new technologies named as "positive molecular attraction", although without any electronic component inside the box. In that manner, companies like Minnesota Global Inc., Quadro Corp, Lil' Orbits, DKL… were distributing some quite similar devices called "**Golfinder**", "**Scantrak 18**", "**GBF**"… until they all were banned by the US legal system.

Approximately at the same time, Quadro Corporation developed the "**QUADRO TRACKER**", a "positive molecular locator" allegedly able to find lost golf balls, illegal narcotics, weapons and explosives, or even missing persons/animals (dogs), depending on the feed in the "carbo-crystalized signature card" which had been tuned to the "identical frequency modulation" as the object you were searching for; the company was sentenced for fraud in 1996. The tool was named as **"QRS 250 G**" for substances, and "**QRS 550 DL**" for dogs, as an example.

The heritage from those fake detectors was passed to the "**MOLE**" Programmable Detection System, produced by a British company called Global Technical Ltd, and based on "molecular resonance" technology, which included a card reader; the tests were absolutely unsuccessful, so the production ceased in 2002.

After the previously shown products, there were some other alleged explosives and drugs detectors whose designers, producers, and/or distributors were arrested, detained and convicted for fraud.

The "**ALPHA 6**" was produced by Comstrac Ltd. / Scandec Inc. / NMS International as a "molecular magnetic resonance" based detector with a card containing the substance feed attached to the handle. Its appearance was quite similar to "Quadro Tracker" and its clones, the same that "**ADE-100**" offered by ASTC UK as their basic and introductory model.

ASTC UK was further distributing the "**ADE 101**" based on "electrostatic attraction" technology, along with other more advanced versions like "**ADE 650**" and "**ADE 651**"/"**GADE 651**", those presently based on "ionic electrostatic attraction".

Figure 3: "ADE 101", "ADE 650" & "ADE 651" models by ASTC. *(Source: http://www.bbc.com/news/uk-29459896)*

Figure 4: "GT200" device sold to Thailand. *(Source: http://www.bangkokpost.com/print/346834/)*

Finally, the "**GT200**" Remote Substance Detection System as distributed by Global Technical Ltd. was shown as ineffective during several official tests, although allegedly functioning through "para/diamagnetism" with the support of specific cards for each substance.

It was assured by the producer of "ADE 651" that the device was truly based on nuclear quadrupole resonance technologies, as evidenced by a Romanian scientist who had written journal articles on that theory and accordingly testified at the trial; he even submitted a patent application to the Romanian Patent Office in Bucharest. The main problem for him was the absolute lack of components able to drive the referred theory inside the devices he made by himself.

MAYBE A NEVER-ENDING STORY; SUSPICIOUS DETECTORS ARE SPREAD ALL AROUND THE MARKET… YET.

Unfortunately, devices like the "ADE 651" and the "GT200" have been recently seen in the hands of Lebanese security officers, members of Libya National Army, police in Egypt and Pakistan, among other countries. In that manner, we could find available in the public market a lot of explosives detectors potentially or clearly based on similar technologies as already described , although there is no judicially-confirmed evidence about their fraud, or strongly tested inefficiency. They are;

"**H3Tec**" (H3 Tec LLC) a long-range locator (LRL) based on "nano-ionic resonance", and offered as a detector of explosives, drugs, minerals, hydrocarbons… but not scientifically tested.

"**PSD-22**" (Programmable Substance Detector) by Intelligence Counter Security & Surveillance Ltd.; the company was not clearly indicating the inspiring technology, although it was not exactly publicized as an explosives detector but "early warning indicator and direction finder ".

"**Mole GT200/Moore GT200**" (MOORE, HUNAN-Jin Industrial Co., Ltd and other distributors), extremely similar device to "MOLE PDS", it was offered in different versions (E, F, ED…) and with different commercial names (UK80M200DTS, M9-MOLE302).

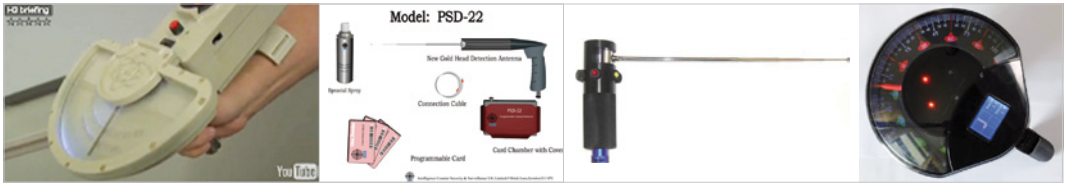


Figure 5: Pictures of some of the referred devices; "H3Tec", "PSD-22", "XK 9" & "Sparkeye RL". (Distribution sources)

"**AL-6D**" (Diodo Bell.), it was distributed as an "explosives, ammunition and unexploded ordnance detector" including nuclear weapons…

"**GT200 ED**" (Shenzhen Smile Electric Co., Ltd. / Bai yuan Yong tai International Technology and Trade (Beijing) Co., Ltd.), Chinese product allegedly based on "molecular resonance".

"**H-MOLE EC900FT**" (I68.com, HC360.com.), another Chinese product distributed by Alibaba and apparently based on magnetic resonance imaging (MRI) and Coulomb's inverse-square law.

"**XK 9**" (SAE Systems Ltd. / CapPeter.), a device based on electrostatic detection, whose Irish creator was arrested and accused of fraud in the United Kingdom in 2012.

"**Sparkeye RL**" or "M103778" (Shenzhen Smile Electronics Co. Ltd. et al.), distributed in some different versions (RL-I to RL-8), it was said to be based on "Terahertz radiation & molecular spectrum vibration".

"**FENNEK**" *(Algerian Centre de Recherche et Développement CRD)*, a device apparently based on ADE's principles was researched and developed in Algerian government facilities, and then evidenced as a fraud.

"**RS-II Remote Sensor"** (Shtiance.com.), based on magnetic cards for each substance, it is shown as a product designed in Canada by its sellers.

It is relevant to highlight that Pakistan's Airport Security Force (ASF) took over making and selling its own explosives detector/wands from 2009. The ASF is technically a civilian institution but is staffed by many serving senior officers deputed from the military. The devices are named "Khoji" (finder), and used by security personnel to protect airports and government installations, and have also been widely sold to the private sector and deployed at malls, hotels and fast-food chains. The device claims an accuracy level of 90 percent, according to a copy of its user manual, based on the principles of "*radiesthesia*", or dowsing. *"Khoji is the first device of its kind that can detect explosives from distances of up to 100 metres (330 feet), even when the explosive is hidden behind walls or metal barriers such as buildings or vehicles," the manual said, "It detects the interference between the magnetic field of the earth, the explosive, the device itself and the human body, which allows the device to penetrate and locate even small amounts of explosives through concrete, soil, and metal barriers." (http://tribune.com.pk/story/1157879/pakistans-bogus-bomb-detectors-business-despite-global-scandal/)*

In India, Brio Macro Security Private Limited is distributing the "MSRED" Remote Explosives Detector, just a device extremely similar to the GT200. It is said to *"… set standards for ion detection. It is extremely easy to operate and delivers fast detection of the programmed substances in a small lightweight package. The features include reduced 'false-positive' readings on contaminated targets."*

There are also other strange devices based on similar technologies of detection, claiming to be able to find things other than explosives;

"**DKL Lifeguard**" (DielectroKinetic Laboratories LLP / DKL International Inc.),they were based on di-electrophoresis force and not specifically marketed as explosives detectors but "living beings detectors"; official blind tests and device analysis did show no high effectiveness nor scientific performance. Three different versions (1, 2, 3) were produced.

"**C-Fast Field Advanced Screening Tool**" (Government of Egypt, Ministry of Defense) , the "molecule-signature" theory-based device was publicised as able to detect Hepatitis C viruses and

Figure 6: Pictures of some detectors locally produced and distributed in Pakistan. *(Sources: ASF/AFP)*

other bacteria, but the patent application said that it could be able to detect explosives and drugs as well.

BRINGING FAITH TO THE FAITHLESS, AND DOUBT TO THE FAITHFUL…

Just reciting Paul Tillich, it looks like the doubt should prevail over the faith when considering the referenced kinds of explosives detectors, and their potential effectiveness and proficiency.

Meanwhile and prudently, we may consider some examples of those devices whose non-effectiveness or effectiveness are already not fully assured, but currently they could be legally distributed and purchased, although it looks like none of the manufacturers and distributing agencies were able to scientifically prove their marketing claims related to detection performance. They are:

"**SNIFFEX**" Is composed of a metal handle, an attached telescopic antenna, and contains two magnets plus a "secret" component. The device is supposed to be able to detect abnormally high concentrations of nitrous oxide radicals. According to the company, it can detect explosives up to 300 meters away by reading the "interference between the magnetic field of the earth, the explosive, the device itself and the human body." The 2005 tests performed by US Naval Explosive Ordnance Disposal technology Division was not really favorable, while the German Federal Criminal Police Office (BKA) officially and negatively reported the effectiveness of the device after a proficiency test and demonstration held in Germany in the same year, 2005.

"**SNIFFEXPlus**" Almost the same device, but it is said to have been improved.

Figure 7: SNIFFEX® & SNNIFEX®PLUS devices.

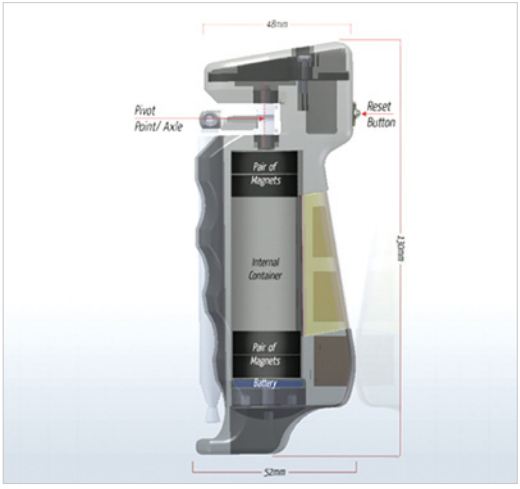


Figure 8: HEDD®1.

"**HEDD®1**" Handheld Explosive Detection Device 1 is said to emit a "*Modulated Magnetic Field (MMF)*" powered with a single 1,55V electric source *"based on its unique patented Magneto-Electrostatic Detection (MED) method*" through *"interacting with the vertical component of the earth's magnetic field creates the conditions for detection of chemical compounds, containing -NO2 / -NO3 and O-. The magnetic field that is modulated from HEDD®1 is tuned for this "bond-/vibrational energy and no other substances will be detected from the device. The conductivity/ bi-polarity of the human body is needed to operate the device. The detection of explosives is achieved with the cross bearing method/triangulation.*" Some functioning tests performed in Thailand were unsuccessful, and the owner of the company was accused of commercial fraud in 2015 in Germany, although the case was closed without any court proceedings. Nowadays, non-officially tested versions of SNIFFEX®PLUS (3rd generation) and HEDD®1 (4th generation) are offered by the distributor.

So in full agreement with C-IED Centre of Excellence reports, we could assert that most (if not all) of those devices "have no functional components"; so in principle, they cannot fully effectively detect explosives. *"Due to the absence of scientifically proven methods of operation, unclear results after several tests of the device conducted by different agencies and organizations, and related reports, the NATO C-IED Centre of Excellence Defeat the Device Branch dissociates itself from the companies' declarations of detection capability, reliability, accuracy*"… please take care when evaluating detectors for acquisition! ■

"Fraud is the daughter of greed."
(Jonathan Gash, in his book
"The Great California Game", published in 1992)

MAIN REFERENCES

- "Fake Detectors Report", C-IED CoE, September 2016, Madrid
- http://www.vanityfair.com/news/2015/06/fake-bomb-detectors-iraq
- https://7our.wordpress.com/2015/09/21/drs-ca-sent-la-fin-du-fennek/
- http://maritimeaccident.org/tags/hedd1/
- http://www.geotech1.com/
- http://lonjho.blogspot.com.es/
- http://sites.google.com/site/sniffexquestions/sniffex/Home/NavyReportfromProPublica.pdf?attredirects=0

Disclaimer

This article does not represent the point of view of any national or multinational organization. Its content should only be considered as the author's opinion.

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. 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), Republic of Ecuador, Iraq and Uganda. ***Email: jrufas@ciedcoe.org***

EXPLOSIVES TRACE DETECTION: CRITICAL COMPARISON OF TECHNOLOGICAL SOLUTIONS FOR OPERATORS

By Simon O. Williams, BA, LLM, Managing Director, Tactique Services

Terrorist elements around the world continue to deploy improvised explosive devices (IEDs) as their most deadly weapon of choice in today's battlespace, posing serious threat to high value targets, such as embassies, hotels, oil-and-gas assets, shopping malls, and transportation infrastructure like airports and seaports.

Advanced explosive detection operations utilize technological solutions in a non-destructive inspection process to determine whether an object, vehicle, or person may contain or possess explosive material or have previously been in contact with explosive material. Bulk and trace explosive detection is commonly used by airports, seaports, and by other security forces, and is increasingly being adopted by users in the private sector.

This article will explore the various types of technology on the market to provide procurement officers and operators with an overview of explosives detection solutions which may complement their activities.

Before examining the solutions, however, it is pertinent to define the threat which IEDs pose in the contemporary paradigm. IEDs are devices designed to cause death or injury by using explosives alone or in combination with toxic chemicals, biological toxins, radiological material, and/or shrapnel. IEDs can be produced in varying sizes, function, containers, and delivery methods. One of the most dangerous delivery methods is the Vehicle Borne IED (VBIED). The devices can utilize commercial or military explosives, homemade explosives, or military ordnance and ordnance components concealed within a vehicle, package, bag, hidden in the ground or in a building, or on a person and can cause devastating destruction resulting from the mass of the explosives and the close proximity in which the IED can access target(s).

IEDs are composed of four parts: Power source, Initiator, Explosive, and Switch. While many well-known security technologies are deployed to identify IEDs as a whole in bulk, simply attempting to detect threats using metal detectors or bulk visualization

An improvised explosive device (IED) attack is the use of a "homemade" bomb and/or destructive device to destroy, incapacitate, harass, or distract. IEDs are used by criminals, vandals, terrorists, suicide bombers, and insurgents. Because they are improvised, IEDs can come in many forms, ranging from a small pipe bomb to a sophisticated device capable of causing massive damage and loss of life. IEDs can be delivered in a vehicle; carried, placed, or thrown by a person; delivered in a package; or concealed on a roadside or in a building.

tools can prove ineffective. This is especially the case in high throughput cargo screening environments such as baggage or mail processing facilities at an airport or a vehicle checkpoint in a heavy traffic location like a hotel or seaport. Seeking non-explosive components of an IED (power source, initiator, and switch) in such environments is like looking for a needle in a haystack. But searching for, detecting, and identifying the explosive component of the IED provides a more practical and effective solution if the right tools are correctly employed.

The majority of IEDs incorporate explosive materials from nitro groups such as nitroaromatic explosives, nitrate ester and nitramine explosives, inorganic nitrate based explosives, chlorate based explosives, and peroxide based explosives.

Targeting the explosive trace of an IED in either particulate or vapor form is possible because most explosive materials emit vapor or gas as they decompose at the molecular level. Similarly explosive material that is handled by a person often leaves a residual trace on that person's hands, clothing, or bag. The trace can be passed on by secondary contact to other objects, such as their shoelaces, belt, door handles, zipper of a bag, or steering wheel of a vehicle, among other items which that person may have touched minutes or hours after handling explosive material.

The fact that explosive traces can be left on objects and persons opens up a wide opportunity for technological solutions to detect such traces in order to identify otherwise innocuous objects, vehicles, or persons as suspicious and justify a diversion of resources to conduct necessary screening.

Capable of detecting the slightest vapor and particulate explosives and chemical traces using sample-swipe techniques and contactless vapor detection, explosives trace detection (ETD) solutions are ideal for a range of customer needs, including and especially airports, seaports, diplomatic security personnel, and security companies tasked with screening cargo, protecting transportation assets, critical infrastructure, and oil & gas installations.

Most commonly known is the ubiquitous K9 bomb-sniffing dog. K9 assets continue to provide a unique and high-demand service in the Counter-IED environment where dogs are trained to detect explosive vapor. However, new technologies have been developed to effectively screen facilities, personnel, cargo, and transportation assets to detect such trace amounts of explosives along with toxic industrial chemicals, and other components which may be part of an IED. Some devices can also identify the chemical composition of the substance on a molecular level, and serve more robustly and continuously in the field than K9 assets can.

... WHILE TECHNOLOGY MAY PROVIDE SIMILAR AND OVERLAPPING SOLUTIONS TO K9s, SPECIALIZED EQUIPMENT SHOULD BE CONSIDERED AN ASSET TO AUGMENT RATHER THAN REPLACE THE USE OF K9s IN TODAY'S OPERATING ENVIRONMENT ...

While technology may provide similar and overlapping solutions to K9s, specialized equipment should be considered an asset to augment rather than replace the use of K9s in today's operating environment. K9s still provide a specialized service and are a tremendous force multiplier in terms of their deterrent effect, mobility, and speed of operation –able to screen a larger quantity of targets in shorter time than a human operator with an ETD device. Yet, K9s can only be trained to detect approximately 10 odors effectively, while ETD devices, on the other hand, can detect a much wider range of threats including numerous types of explosives, as well as toxic industrial chemicals, and even narcotics. Some devices have threat libraries in the hundreds or thousands, and these libraries can be modified and expanded with simple software updates.

BULK DETECTION

Bulk detection seeks to identify actual explosive material present in a package, container, person, vehicle, or other object. Bulk detection methods are less dependent on sample collection than trace detection methods, and are not affected by the presence of an explosive background. However, equipment costs associated with bulk detection are often higher, and these units are generally floor based and not mobile. Some bulk detection techniques – especially those based on imaging, such as X-ray imaging – may have a lower degree of specificity than trace detection methods.

As a result, many operators, including those outside of the aviation environment are turning to trace detection to augment or support their Counter-IED posture. While it is, of course, ideal to have access to both trace and bulk explosives detection methods, as they possess complementary strengths, the feasibility of having both solutions simultaneously available is usually constrained by cost and by the operational needs of the facility or the security provider. Moreover, various trace detection solutions have been produced in handheld systems increasing the versatility of the product for field deployment.

... MANY OPERATORS, INCLUDING THOSE OUTSIDE OF THE AVIATION ENVIRONMENT ARE TURNING TO TRACE DETECTION TO AUGMENT OR SUPPORT THEIR COUNTER-IED POSTURE ...

TRACE DETECTION

Trace detection determines the presence of explosive material or contact with explosive material by detecting the presence of microscopic residues of explosives, either as particles or as vapor (gas-phase molecules) in the sample area.

The term “trace detection” refers to both vapor and particulate trace detection:

- *Vapor* – Gas-phase molecules that are emitted from a solid or liquid explosive. The concentration of explosives in the air is directly correlated to the vapor pressure of the explosive material and to other factors such as the amount of time the explosive material is present in a location, its packaging, air circulation in the location, and other circumstantial and environmental factors.
- *Particulate* – Microscopic particles of the solid explosive material that adhere to surfaces (directly from contact with the explosive, or indirectly, through contact with someone’s hands who has been handling explosives.)

The trace detection process involves using a sample swab or vapor trace detector to screen a small sample area for explosive residue allowing an operator to determine if the subject contaminated from handling or being in proximity to explosives materials. This may reveal their earlier contact with explosives, or may even lead to discovery of a bulk source. For example, if a terrorist with explosives hidden in his vehicle is screened by trace detection equipment, the trace amounts of the explosives present on the terrorist’s skin or passed on to the clothing, door handle, or steering wheel from earlier handling of the IED when placing it in his vehicle will likely trigger an alarm on the ETD device. Thus, further resources can then be allocated to search the individual and his vehicle fully, and the IED can be found and disabled.

Cautious handling of the IED’s explosives components by the perpetrator and sufficient use of disposable gloves may reduce the extent of particulate contamination or residue. However, even with such precautions, completely eliminating detectable amounts of contamination and residue is very rare. Most IED constructors and carriers will not have the expertise, time, or financial resources available to manufacture and move their IED without coming into contact with the explosive component or residue thereof. As a result, contamination is highly likely on the perpetrator, his concealment objects, and methods

of transport resulting in wide applications for the particulate method of sampling.

Due to such success of particulate sampling, the detection of trace amounts of explosive does not necessarily reveal the presence of an IED. An alarm from ETD equipment may indicate the presence of vapors from or particles of explosive material which were previously in contact with subject sample. So if that same person in the example above placed explosives in another person's vehicle or left an explosive package at another facility, he may still trigger the trace detection alarm due to explosive traces on his skin, clothing, or vehicle although the IED is no longer in his possession. Furthermore, it is important to mention that trace-detection techniques may be vulnerable to unsophisticated countermeasures, and the absence of trace amounts of an explosive does not completely guarantee that no explosive is concealed.

... IT IS IMPORTANT TO MENTION THAT TRACE-DETECTION TECHNIQUES MAY BE VULNERABLE TO UNSOPHISTICATED COUNTERMEASURES, AND THE ABSENCE OF TRACE AMOUNTS OF AN EXPLOSIVE DOES NOT COMPLETELY GUARANTEE THAT NO EXPLOSIVE IS CONCEALED…

Various technological solutions have been developed to detect such trace signatures for explosive materials. The strength of the explosive signature detected by the equipment is not related to the quantity of explosives present. Trace detection techniques are less likely than bulk detection techniques to misidentify common, nonthreat items as explosive materials, however, they may occasionally suffer from missed detections due to inadequate, improper, or incomplete sample collection. The following are some types of ETD solutions which are being manufactured and deployed commercially:

Colorimetrics

The use of Colorimetric test kits for explosive detection is one of the oldest, simplest, and is still a widely-used method for the detection of explosives. Colorimetric detection of explosives involves applying a chemical agent to an unknown material or sample and observing a color reaction. These reactions can be conducted using analog agents in liquid or spray form, or in more technical electronic or automated digital systems. Common color reactions are cross-referenced electronically or to a chart, indicating to the user if explosive material is present, and in some cases, may even identify the type of explosive group from which the material is derived.

Ion Mobility Spectrometry (IMS)

Ion mobility spectrometry (IMS) is the most common technique used for commercial applications of explosives trace detection. IMS instruments can operate in swipe (particulate) and/or vapor detection modes. Contaminants in the sample are ionized, usually by a radioactive source which emits low-energy electrons. The ions are accelerated by an electric field and then traverse toward an ion detector. The time it takes the ionized contaminant to traverse the distance is unique for each substance. Therefore, measuring the elapsed time can serve as a means of identification, allowing the ETD device to determine the substance's classification. Analysis times can range from several seconds to a few minutes. If explosives are present, the negative ions typically associated with the explosives are recognized and the device alarms as a threat.

Thermo-Redox

Thermo-redox technology is an electrochemical technique based on the thermal decomposition of explosive molecules and the subsequent reduction of NO^2 groups. A sample is drawn into the system and is passed through a concentrator tube, which selectively traps explosive-like materials. The sample

is heated rapidly to release NO^2 molecules, and these molecules are detected using proprietary technology. This solution, however, can only detect the presence of NO^2.

Chemiluminescence

Chemiluminescence is the production and emission of light that occurs as a product of a chemical reaction(s). Most common explosives materials contain nitrogen (N) in the form of either nitro (NO^2) or nitrate (NO^3) groups. Additionally, most explosive materials used in plastic explosives also contain NO^2 groups. The most commonly used chemiluminescence reaction scheme for explosives detection involves infrared radiation (IR) light emission from excited-state nitrogen compounds. The produced IR light is directly proportional to the amount of NO present, which is related to the amount of the original nitrogen-containing explosive material that was present.

Multi-channel Fluorescence Technology

Similar to chemiluminescence, trace particulate samples are heated within the ETD device to vaporize a sample. Then an internal pump pulls the vapor phase molecules across the suite of sensing materials. These sensing materials interact with molecules in the sample, causing a change in light intensity that is measured by the device. According to manufacturers of this solution, an explosive is "sensed" when the light output of the sensing material changes in a specific manner as response to explosives in the sample. The change in intensity of light output is measured by extremely sensitive detectors consisting of many fluorescent molecules linked together to form a chain. These molecules communicate with each other electronically, so that when any one of the molecules in the wire interacts with a molecule of explosive, all the molecules in the chain cease emitting light. A single explosive molecule switches off the fluorescence of multiple fluorescent molecules in the chain. As a result, an extremely small amount of explosive material can trigger a measurable reduction in light output, allowing the ETD device to determine the identity or class of the explosive.

Mass Spectrometry

Mass spectrometry (MS) analyzes an explosive material's molecular weight and fragmentation patterns for identification. While there are different types of mass spectrometers, the principle of the technology involves mass filtering. In this process, molecules are ionized and passed through a filter, which allows ions to be measured based on their charge-to-mass ratio. These measurements can often be used to calculate the exact molecular weight of the sample components which is then cross-referenced with the ETD device's software library to identify the unknown compound by its determined molecular weight. ■

ABOUT THE AUTHOR

Simon O. Williams, BA, LL.M is the managing director of Tactique Services (USA). His company provides advisory, logistics and risk management solutions for the global transportation and petroleum sectors, specifically offering innovative equipment, training, and consulting on explosives detection for clients operating in high risk countries (www.tactique.org).

Williams holds a BA from the University College London and a LL.M from the University of Tromsø in Norway.

DENSITY RANGES OF EXPLOSIVES FOR DEVELOPING X-RAY DETECTION WINDOWS

By John D. Howell, DSA Detection

Everyone is familiar with the long lines associated with a busy security checkpoint. With advances in technology, checkpoints today contain any number of screening devices, which include cabinet X-rays, portable X-rays, walk-through metal detectors, hand-held metal detectors, explosive/narcotic trace detection instruments, bottle liquid scanners, etc. One of the major pressures security supervisors face is the responsibility to streamline throughput; i.e. speed up the entire checkpoint operation. One of the first potentials they will look at is how to improve the automatic detection capabilities of their instruments. For checkpoints utilizing cabinet x-ray systems, a major topic of interest is how to avoid automatic detection alarms occurring on mundane, non-threat items. Automatic detection density windows can be adjusted to reduce false alarm rates and increase throughput. Extensive research on this topic combined with my own experience in this field leads me to believe that narrowing explosives detection windows to reduce false alarm rates does not streamline an effective checkpoint screening operation.

OVERVIEW

A full analysis was performed on peer-written technical essays to determine the density range believed to cover explosives. Then, exact density values from 8 of the most common explosive manufacturers themselves were gathered and organized for analysis. These subjects were compared to examine both the current knowledge level in the threat detection field and to identify the truest density window for explosives.

After these findings, a full experiment was conducted using items known to routinely cause false alarms in security checkpoint x-rays due to their similarity in density to real explosives. The following common items were examined: shampoo, soda, water-based products, bar soap, hair conditioner, hand lotion, hair gels, body wash, and paper (stacked). The purpose of this experiment was to see how close these common items were to the detection ranges of the machines, and if the machine would be able to differentiate the two. This would potentially assist in determining any potential benefits and/or consequences of narrowing detection windows to reduce false alarm rates.

A common question regarding this subject is whether or not one can effectively combine explosive density settings with size discrimination to increase throughput. To answer this with data, the harmful range of blast pressure on humans was examined, along with how blast calculators are used to determine blast pressures of any given explosive by using its net explosive weight and size range. This data was analyzed to determine reliability when compared with variables and the technical capabilities of X-ray instruments today.

The final results of this study in its entirety would then be compared with master security screening, explosive ordnance, and X-ray instrument knowledge to examine the benefits and risks associated with adjusting automatic detection windows to reduce false alarms and increase throughput.

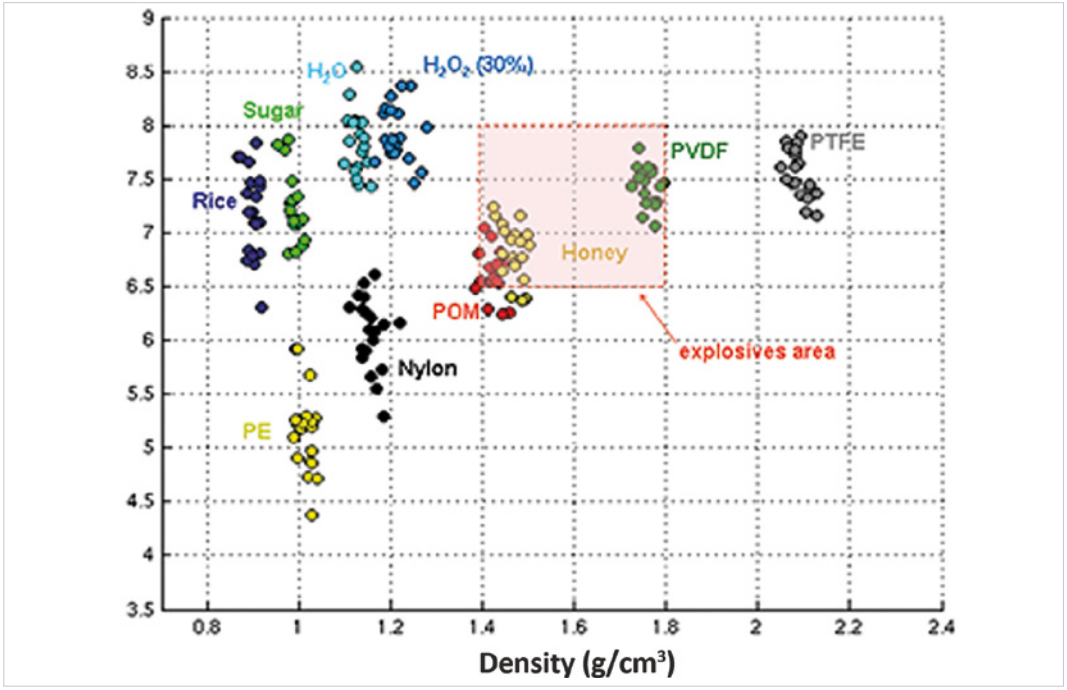


Figure 1. [2]

RESULTS

All of the technical papers found seemed to focus only in the very high density ranges of explosives (Figure 1).

The widely-accepted density range for explosive material, based on charts, graphs, and papers on the topic was found to be extremely inaccurate. The reason for this appeared to be that the density range was a result of data based on only some explosives rather than all. Compared with EOD technician experience and explosive simulant development, the majority of explosives (those with density values below 1.2 g/cc) are left out of these higher-density windows, compromising their accuracy. The common density window, intended to represent explosives as a whole, ranged from about 1.2-1.6 g/cc and sometimes notably higher from 1.4-1.8 g/cc (Fig. 1)[2]. These charts did not represent enough explosives to be considered accurate, since the density of most explosives falls below 1.2 g/cc.

The question inevitably rose as to where this source information had been collected and why incomplete information had been effectively dispersed into scientific essays and presentations. As a result, the perhaps most popular online research center was consulted for comparison – Wikipedia. The range for explosive densities provided on the Wikipedia page lists only 2-3 explosives below 1.1 g/cc, with all of the others above 1.2 g/cc. Their data is not incorrect but rather extremely limiting, appearing to focus solely on well-known main charge explosives such as TNT, C-4, etc. This almost perfectly matches all of the other charts found in my research.

Actual material safety data sheets (MSDS) and safety data sheets (SDS) from real explosives on the market were then sourced, and relative density data was pulled and organized. Current data sheets can be found from all major explosive manufacturers, and they should be updated when the manufacturers change

DYNO
Dyno Nobel

MATERIAL SAFETY DATA SHEET
DYNO NOBEL INC.
11TH FLOOR CROSSROADS TOWER
SALT LAKE CITY, UTAH 84144
PHONE: 801-364-4800 FAX: 801-328-6452
E-MAIL: DNNA.HSE@AM.DYNONOBEL.COM
FOR 24 HOUR EMERGENCY CALL 800-424-9300

MSDS# 1052

DATE: 11/11/03

Supersedes MSDS
1052 05/09/03

SECTION I - PRODUCT IDENTIFICATION

Trade Name(s):
DYNO GOLD® C, DYNOGOLD® C EXTRA
DYNO GOLD® C LITE, DYNO GOLD® C LITE SUPER
DYNO GOLD® CS LITE
DYNO GOLD®, DYNO GOLD® LITE
DYNO GOLD® B, DYNO GOLD® B LITE
HD
1116, 1126P, 1136P, 1146P
IREMEX 362, IREMEX 562, IREMEX 762, IREMEX 764
RJ5
RG1-A
RUG-1 (Canada Only)
DX 5007; DX 5010
TITAN® XL 1000
TITAN® 1000, TITAN® 1000 G

Product Class: Bulk Emulsion
Product Appearance & Odor: Translucent to opaque, viscous liquid. May be silvery in color. May have fuel odor.
DOT Hazard Shipping Description: As Transported:
Oxidizing Liquid, n.o.s. (Ammonium Nitrate) 5.1 UN3139 II
After Blending with Density Control Agent On-site:
Explosive, Blasting, Type E 1.5D UN0332 II

NFPA Hazard Classification: Not Applicable (See Section IV - Special Fire Fighting Procedures)

SECTION II - HAZARDOUS INGREDIENTS

Ingredients:	CAS#	% (Range)	TLV-ACGIH
Ammonium Nitrate	6484-52-2	30-80	No Value Established
Sodium Nitrate	7631-99-4	0-15	No Value Established
Calcium Nitrate	10124-37-5	0-35	No Value Established
Fuel Oil	68476-34-6	0-10	No Value Established
Mineral Oil	64742-35-4	0-7	5 mg/m^3
Aluminum *	7429-90-5	0-5	10 mg/m^3

* The hazardous ingredients marked with an asterisk are not found in the majority of listed products.

Ingredients, other than those mentioned above, as used in this product are not hazardous as defined under current Department of Labor regulations.

SECTION III - PHYSICAL DATA

Boiling Point: Not Applicable

Vapor Pressure: Not Applicable

Vapor Density: (Air = 1) Not Applicable

Density: 0.8 - 1.5 g/cc

Percent Volatile by Volume: <30

Solubility in Water: Nitrate salts are completely soluble, but emulsion dissolution is very slow.

Evaporation Rate (Butyl Acetate = 1): <1

Figure 2: Dyno Nobel MSDS dated 11/2003.

Safety Data Sheet

Odor Threshold	:	Not available
pH	:	Not applicable
Evaporation Rate	:	< 1
Melting Point	:	Not applicable
Freezing Point	:	Not applicable
Boiling Point	:	Not applicable
Flash Point	:	Not applicable
Auto-ignition Temperature	:	Not available
Decomposition Temperature	:	Ammonium nitrate: 210 °C (410 °F)
Flammability (solid, gas)	:	Not applicable
Lower Flammable Limit	:	Not applicable
Upper Flammable Limit	:	Not applicable
Vapor Pressure	:	Not applicable
Relative Vapor Density at 20 °C	:	Not applicable
Relative Density	:	Not applicable
Density	:	0.95 - 1.25 g/cc
Specific Gravity	:	Not applicable
Solubility	:	Partially soluble in water
Partition coefficient: n-octanol/water	:	Not available
Viscosity	:	Not available
Explosive properties	:	Explosive; mass explosion hazard
Explosion Data – Sensitivity to Mechanical Impact	:	Not sensitive
Explosion Data – Sensitivity to Static Discharge	:	Not sensitive

Figure 3: Dyno Nobel SDS dated 3/2015.

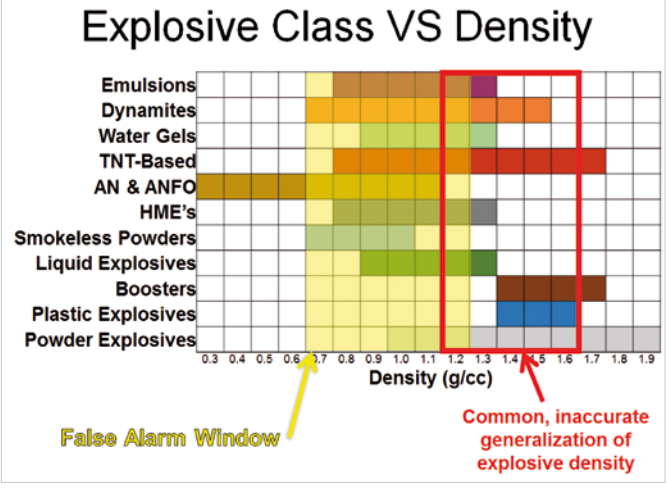


Figure 4: Study and Experiment Results.

their formulas. It was observed that Dyno Nobel had updated their emulsion powder to a relatively lower density than the formula they had previously manufactured and sold in the year 2003 (Fig. 2-3) [1]. In examining almost 500 different explosive products from 8 different explosive manufacturers, it was observed that the resulting density range proved to begin as low as 0.05 g/cc, whereas the common belief remains that it begins around roughly 1.1 g/cc.

Organized based on the data accrued in this study, Figure 4 details the density ranges of several major explosives, the commonly-believed range of explosive density, and the density range of some of the most common items known to falsely alarm as explosives in X-ray instruments.

In regards to the use of size discrimination as a factor in limiting alarms in X-rays, it was noted that the amount of blast pressure to cause critical/terminal injuries was above 40 PSI or 275 Kpa, however unexpected variables will completely alter this data. There was found to be no reliable number due to this. Online blast calculators were observed and can be used to estimate blast pressures of specific explosives of specific sizes. However, a checkpoint must be ready to encounter all explosive types, and the market is continually changing. It should also be noted that X-rays cannot weigh objects; size cutoffs are based solely on surface area analyzed during the X-ray process.

CONCLUSION

All of the data gathered from scientific papers and presentations sourced proved to suggest a Mandela Effect regarding the true density range of explosives. The information being passed around is based on data that does not represent all of the explosives currently utilized on the market, omitting some of the most common explosives in use that are encountered by EOD technicians. The results of this research prove the importance of referring to

the earliest sources of data when understanding the true density window of the explosives category of materials. Changes in explosive formulas and thus densities most frequently occur without warning; therefore it was made apparent that the only way to reliably formulate a density window to represent explosives was by sourcing from current data sheets from explosive manufacturers themselves. In looking at almost 500 explosive products from 8 manufacturers and discovering density levels as low as 0.05 g/cc, it can be assumed that the common window beginning around 1.2 g/cc cannot be relied upon when observing the effectiveness of explosive density windows used in automatic detection of X-ray instruments deployed at security checkpoints.

It is observed in Figure 6 that it is unwise to try to prevent false alarms by lowering the explosive density threshold settings in X-ray instruments. To do so would cancel out any chance of a large array of explosive materials eliciting an explosives automatic detection response.

It is not recommended to lower size windows to prevent alarms of smaller amounts of materials which match the density range of explosives. If those materials were live explosives, they could still cause harm and should never be prevented from detection at a security checkpoint. Since X-rays cannot weigh objects, the size discrimination windows are already limited in ability and should not be limited further.

Personal experience developing explosive simulants and teaching security forces checkpoint operations has proven that explosive automatic detection windows are already limited in their ability to detect explosives. It is neither productive nor safe to further limit their detection ability. The most effective security checkpoint will not render the explosives automatic detection settings less sensitive than the default programmed, and will rather improve training to detect explosive substances and devices on the instruments being utilized at the checkpoint. Automatic detection alarms can never be relied upon to detect all explosives, and false alarms are a necessary aspect of all effective and secure security checkpoints. ■

REFERENCES

[1] "Product Hub." Technical Information & SDS. N.p., n.d. Web. 09 Jan. 2017. <http://www.dynonobel.com/apac/resource-hub/products>.

[2] Rebuffel, Veronique, Jean Rinkel, Joachim Tabary, and Loik Verger. "New Perspectives of X-ray Techniques for Explosive Detection Based on CdTe/CdZnTe Spectrometric Detectors." International Symposium on Digital Industrial Radiology and Computed Tomography. Germany, Berlin. 20-22 June 2011. Web. 15 Jan. 2016. <http://www.dir2011.com/Portals/dir2011/BB/we21.pdf>.

ACKNOWLEDGEMENTS

Dyno Nobel
Austin Powder
Orica
Kapeks
Ensign Brickford
BIAFO (manufacturer of TOVEX)
Explosiva (manufacturer of SEMTEX)
Mondial Defense

ABOUT THE AUTHOR

John Howell, Director of Explosives Technology.

John has worked in the government security and national defense industry for over 27 years. John was formerly with the U.S. Marshals Judicial Security Division where his responsibilities encompassed all aspects of contract oversight (COR/COTR) and training of Court Security Officer at FLETC on screening operations. From 1999-2007, John worked for the Department of State, Bureau of Diplomatic Security's Explosive Detection Program and Explosives Countermeasure Unit, as well as a COTR and Program manager of training. From 1987 to 1999, John was an Explosive Ordinance Disposal Technician with the U.S. Marines. He is a Combat Vet of the first Gulf War. John also served 4 years from 2007-2011 in the Army NG 753 EOD unit as the training NCOIC.

Insurgents in North East India.
Source: www.nelive.in

IEDs: ATTACK THE NETWORKS - NEED FOR MULTI-AGENCY COORDINATED EFFORT

By Colonel H R Naidu Gade (Retd.)

INTRODUCTION

India, a vibrant democracy and nation with great diversity, is beset with many internal security challenges since its independence, manifesting as insurgencies in the North Eastern States, Militancy in the States of Punjab and Jammu & Kashmir, Maoist menace in the 'Red Corridor', foreign sponsored/home grown terrorism, large scale riots and violent agitations on many social issues. These hostile elements have extensively used IEDs as the weapons of choice against the security forces and the civil population. Over a period of time, numerous threat networks have emerged which adopt, fund, support and sustain insurgencies, militancy and terrorism. They operate mostly independently and sometimes in consonance complementing each other's resources and modus operandi. The four basic elements of C-IED Operations: Attack the Network; Prepare the Force; Defeat the Device; and Exploit the Incidence, when carried out with perseverance, consistency and good coordination would result in long term relief from the IED menace. Attack the Networks operations, in addition to 'nipping in the bud' the designs and intentions of the hostile elements, also would considerably destroy and diminish their capacities in the long term.

ATTACK THE NETWORK

Attack the Network, a firm and decisive endeavour, enables offensive operations against complex

Kashmir militants. Source: www.zeenews.india.com

networks of adversaries, their financiers, leadership, ideology, communications, logistics, intelligence set up, IED makers, trainers and supporting infrastructure by providing hard intelligence, surveillance, reconnaissance, information operations, targeting, biometrics and weapons technical intelligence capabilities to the C-IED forces. Attack the Network activities require a balanced set of lethal actions against adversary networks and non-lethal actions directed at the threat. It also requires friendly and neutral networks to undermine adversary networks or to reduce or eliminate the factors that allow threat networks to operate. Attack the Network actions require a common and consistent operational framework built on three tactical areas: gain valuable and hard intelligence, build relationships with all stake holders, and finally neutralize the threat networks. This also requires a coordinated and inter-agency approach and consists of largely offensive and proactive measures, driven by intelligence that may go beyond the areas of actual operations, designed to disrupt the networks of the adversary's IED systems.

Intelligence Gathering

Hard actionable intelligence enables C-IED operatives to undertake more precise attacks on the networks employing and supporting IED attacks. The Central and State's intelligence agencies at all levels should work in coordination and willingness to share intelligence for meeting the operational needs of C-IED forces. Intelligence, Operations, Technology adaptation and Logistics should work in unison and synergy for effective and successful C-IED operations. High-value individuals within the threat networks, transnational IED facilitators operating globally and IED makers or trainers need to be identified and their activities monitored continuously. The intelligence personnel should be embedded with C-IED units fighting the hostile elements to provide inputs for deeper analytical capabilities at the higher echelons of fighting formations and at the states and the national level. Develop tools for decision support and inter-agency target-management which will provide a matrix of inter-agency and eventually national capabilities aligned to entities of interest and provide a dashboard

Bomb maker. Source: www.wired.com

showing the status of those capabilities against given targets of interest. Collect various forms of intelligence from different organisations and departments through user input to allow analysts to track specific entities. Put in place an all-source methodology designed to link specific insurgents to specific IED events while leveraging disparate data sets and tools. Intelligence analysts should take up case studies that identified previously unknown network affiliations to IED attacks across the country. The all-source methodology over time will provide better reliability on IED network signatures and help prioritize networks based on their connection to IED attacks. Establish special programs to vet and manage initiatives for rapid fielding of materiel and non-materiel technologies, giving full collection, exploitation and analytic (electronic intelligence, human intelligence, and communications intelligence) advantage to the security forces in attacking IED networks. Employ pattern analysis, an effective way to increase prediction accuracy on future events. At the tactical level gather intelligence on the location, tactical characterization and technical categorization of IEDs, the identities of people participating in the adversary network, the location and sources of their supplies and funding, and ways to influence people from participating in adversary networks. The intelligence gathered needs to be retained, shared and transferred across the area of operations.

Obtain Weapons Technical Intelligence (WTI) derived from the processes and capabilities that collect, exploit and analyse asymmetric threat weapons systems to enable Force protection, Targeting, Sourcing and

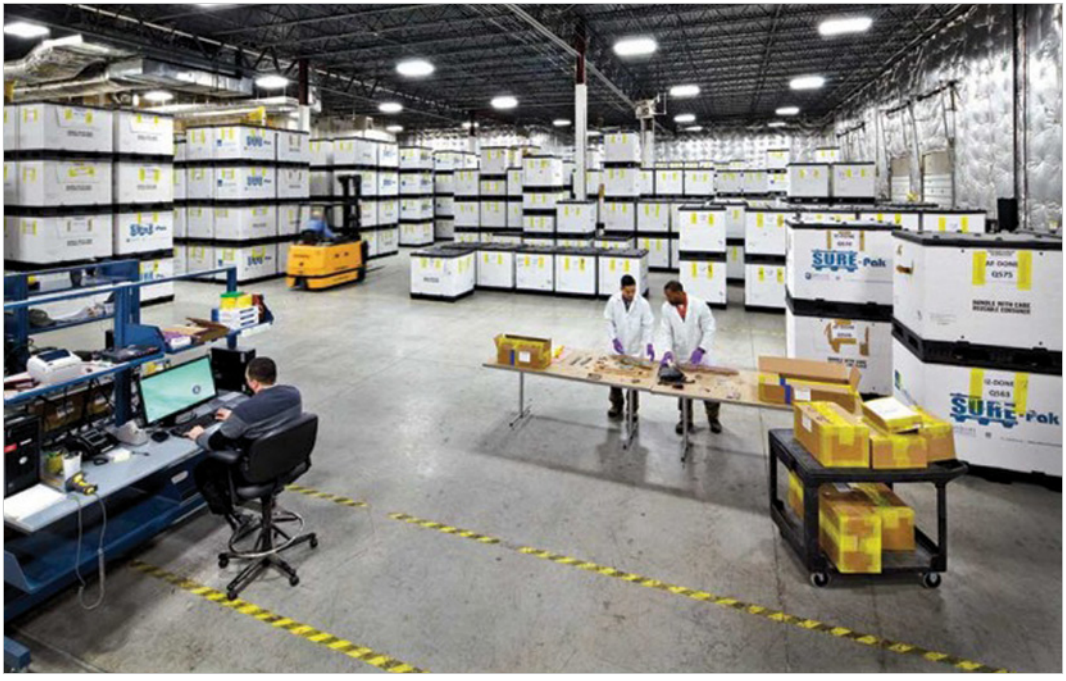
Terror finance. Source: www.trackingterrorism.org

Support to prosecution: Force protection informs the security forces of emerging threats; facilitates research & development; validates threats for testing; and documents electronic, physical or event signatures. Targeting distributes knowledge, analyses and predicts patterns, maps devices to a group or person, analyses links and networks, as well as conducts all-source fusion. Sourcing identifies national or transnational sponsorships, tracks component movement, identifies manufacturing process, and identifies network leadership and financing. Support to prosecution matches individuals with a place, device, event, paraphernalia and/or weapon; and compiles a forensic examination of latent prints, DNA, tool marks, assembler patterns and trace evidence. The WTI exploitation process levels involve tactical examination of WTI physical material from one event; Operational forensic examination as material and data in the theatre; and Strategic scientific examination of material and data from an event, identifying associations between events and/or people. Incorporate WTI into the overall intelligence cycle.

Building Relationships and Cooperation

The inter-agency cooperation and building relationships with friendly and neutral networks would support efforts to highlight IED supply chains and reveal the nature,

IED components. Source: www.LinkedIn.com



Bomb Warehouse. Source: www.bloomberg.com

type and location of IED networks. Hence, inter-agency partnership needs to be developed and strengthened among the security forces, intelligence organisations, law enforcement agencies, regulatory bodies, chemical industry and other government organizations to identify networks responsible for the procurement, transport, distribution and employment of IED components. The partnership must build and operate a classified network to share data, collaborate on intelligence products and plan dynamic and static operations by security forces against facilitation networks. The Ad hoc Multi- Agency Centres presently functioning both at the Centre and at the States must be strengthened and made to operate full time. Setting up of a permanent body like National Counter Terrorism Centre (NCTC) at the national level would facilitate coordination, intelligence and resources sharing, monitoring threat networks, threat based target prioritisation, quick decisions and precise actions. This organization/ consortium of agencies should work to identify targets and disrupt the facilitation networks used by insurgents and terrorists to support attacks on security forces and civilian targets. The consortium must combine data and unique authorities among inter-agency partners to target facilitation networks through dynamic and static operations resulting in disruption of key nodes in insurgent networks. NCTC could play a role of whole-of-government integrator of all C-IED capabilities. The National Bomb Data Centre of the National Security Guard, could function as an Adversary's Explosive Device Analytical Center, and be the primary national facility for processing, exploiting and storing of WTI-related material for use by the security forces, law enforcement agencies, intelligence organisations and the C-IED operatives. Use information operations to build trust and support with local populations and build effective relationships with the right people to gain the cooperation of the local power base. Deep understanding of local culture, building trust through positive actions and reducing collateral damage

IED Forensic laboratory. Source: www.popsci.com

during C-IED operations would help in long lasting and beneficial relationships with the local population. Initiate and genuinely implement civic action programmes to address needs of the locals like roads, electricity, medical aid, water supply and sanitation. Maintain frequent communications with the local power base and local community.

Neutralising Hostile Networks

Eliminate through lethal and non-lethal means the adversary network's ability to operate effectively by co-opting the adversary network, removing the local populace's active & passive support for the adversary network, and disrupting the adversary activities and supplies. Effective and successful neutralisation of hostile networks entails: providing physical security to local population from intimidation and retribution by hostile elements; minimising the drivers of instability through use of non-lethal actions as catalysts for stability and to isolate threat networks from the population; disrupting the adversary network with information operations; seeking out any opportunity to gather intelligence on or disrupt the adversary; portraying the adversary as a detriment to economic prosperity, while promoting economic prosperity; exploiting the success of C-IED operations through demonstrated superiority over the adversary to build the confidence of the locals as partnered forces; destabilising easy supply of IED components and people to the network; determining if any IED supplies are used locally for legitimate uses, If so, support the substitution of a different item where possible; using lethal actions, where necessary, to eliminate key influential nodes in the adversary network; using targeting analysts to develop the adversary network, build targeting packages and identify the information requirements necessary to complete the packages; and focus targeting on the critical vulnerabilities that will have the most impact on the networks affecting the area of operations.

Multiagency Centre. Source: www.economydecoded.com

CONCLUSION

Attack the Network Operations are very intricate and the most critical activity of C-IED operations. Meeting the IED challenges require: dedicated, focused, persistent, and resourced efforts that are operationally proven and time-tested enduring capabilities; rapid anticipation, identification, development, acquisition and fielding of emerging technologies into existing C-IED solutions; fusion and analysis of operations, intelligence and information to sustain scalable analytical capability to provide accurate, time-sensitive information and counter-network support; developing and defining C-IED training standards for forces to build partner capacity; weapons technical intelligence through synchronised efforts to collect, analyse, exploit, and disseminate current and emerging technologies. ■

ABOUT THE AUTHOR

Colonel H R Naidu Gade (Retd.), [B E (Civil), M Sc (Defence Studies), M B A (HR)]

Commissioned in to the Corps of Combat Engineers. A Civil Engineer, Management and Security Professional, with 41 yrs of rich experience (8 years international) in the field of Combat Engineering, Chemical, Biological, Radiological, Nuclear and Explosives (CBRNe) Defence, Security & Disaster Management and Counter-IED Operations. Is a qualified CBRN and C-IED Professional.

Graduate of Defence Services Staff College and Army War College, commanded an Armoured Assault Engineer Regiment. Held important Command, General Staff and Instructional appointments in the Army.

Former Chief CW Inspector for nearly a decade with the 'Organisation for Prohibition of Chemical Weapons (OPCW)', The Netherlands, **winner of the Nobel Peace Prize 2013**. Led teams of international professionals on a large number of verification missions to various member countries, to verify the inventory of Chemical Weapons and monitor their destruction.

Presently the Chief Consultant with **'CBRNe Secure India'** a 'forum' for bringing in awareness in the general public, government and corporate entities on the threats arising from the use of CBRNe material and their disastrous consequences. Has been extensively speaking in various international & domestic conferences on CBRNe and C-IED Issues. Additionally, he contributes articles to many CBRNe and C-IED related journals worldwide.

IED Components.

WEAPONS EXPLOITATION AND POST BLAST SCENE INVESTIGATION TRAINING

By Robert Shaw, Security and Intelligence consultant

Security forces around the world that are operating in conflict or post conflict countries are being targeted by IEDs. The IEDs are used both as a standalone form of attack and with other weapons in complex attacks. IEDs are versatile, cheap, easy to construct, can be emplaced or hidden almost anywhere. They can also use a variety of payloads such as shaped charges, chemical, biological or radiological material to have maximum effect against a range of targets that includes personnel, vehicles and infrastructure.

The use of IEDs against security forces and civilians, in conflict around the globe has produced strategic effects as well as a tactical level influence on tactics, techniques, and procedures and cost nations money and lives. Unfortunately, the enduring successful use of IEDs makes it a weapon system that will constantly develop and be used in future conflicts.

Current military forces across the world are earmarked to be either intervention or adaptable forces. Adaptable forces stabilise the security situation post intervention and then conduct counter- insurgency and host nation capacity building including C-IED activities. Amongst these activities are the clearance of ERW, ammunition and weapon storage management, counter proliferation, IEDD and the intelligence functions of IED network attack. The activity that links the short term force protection element of IEDD and the long term element of attacking the IED network is post blast scene investigation, also known as weapons exploitation, which is carried out by police scenes of crime officers or military weapons exploitation teams (WET).

The WET are part of an exploitation unit that exploit all aspects of recovered forensic evidence including IEDs or parts thereof, weapons, ammunition, electronic or written data, communications equipment and the terrorists themselves. The information gained is then processed into actionable intelligence which drives future operations and can drive changes to the security forces' doctrine, its training and education, the

Explosive theory training on the range.

development of technology and lessons encountered. It also enables the identification and cutting of supply routes by both political engagement and interdiction utilising search or other activities. Therefore, weapons intelligence is very much an enabling activity that has an effect on all other C-IED lines of operation including attack of the IED network. Given its level of importance weapons intelligence teams need to be highly trained and effective, both to ensure legality of forensic evidence and to ensure effective intelligence products are produced in a timely (consistent with safety) manner.

Effective education and training are imperative and the team's capability relies on a well structured and adequately resourced progressive training that initially is at the individual level and then follows with collective training that encompasses the teams, the exploitation unit and the wider C-IED force. All training requires an infrastructure that enables foundation and mission specific elements, the right number of qualified and experienced instructors, a training pool of equipment that reflects the equipment to be used on operations, the time required to train to the required standard, a validation and assurance system, a lessons encountered system and a continuation training or professional development programme. Depending on the complexity of tasks and the equipment used, training to build an effective capability takes time and yet the loss of organisational knowledge can be quite swift so training and education need to be continuous and not just put into place just prior to a deployment.

So what training does the WET need? The training management system used throughout NATO is the Defence Systems Approach to Training (DSAT) which ensures that training meets the criteria of being appropriate, cost effective, efficient, effective and safe. The first stage in this process is analysis where the organisation decides whether the training is a new skill to be taught or an amendment to an existing one. The second stage is the design of the training where it is decided what the training activity will look like; who delivers it and what resources are required. The third stage is the delivery and the fourth stage is the assurance where the organisation looks at whether the training is being delivered correctly, does it meet the requirement and is the whole training system fit for purpose?

Weapons exploitation teams can be military or police personnel or a mix of both. The essential spread of skills across the core team includes a team commander that controls the team during the investigation task, a forensic collection expert responsible for collecting the evidence in a manner conducive with its preservation, an explosives expert (IEDD operator responsible for triage of the IED components and explosives safety), and an intelligence expert responsible for analysis of the scene, the context of the attack and the interviewing of witnesses. The intelligence analyst will be responsible for drafting the task report. The team cannot go unsupported in a high threat environment and might complete its investigation as part of a larger response force that should provide force protection and preservation of the scene (providing the cordon and controlling access) whilst the task is in progress and the scene is exploited. The force protection force should also handle any detainees and carry out on

Afghan weapons exploitation team (WET).

scene tactical questioning and processing. The team will need to be supported by medical assistance unless one of the WET is cross trained.

The WET training normally encompasses the exploitation process and functions within the deployment country, which levels of exploitation are present and what their capabilities are. The processes and functions will also include the tasking authority and reporting chain, including its timings (an initial 'first look' report is normally compiled and disseminated within 12 hours; a full and more detailed report within 24 hours). Training will also include the history of terrorism and the use of IEDs from a global point of view and then goes into more detail on the terrorist group(s) within the intended deployment area, their weapon systems (both conventional and improvised) and TTPs. This is will include the terrorists' group organisational structure, how they are resourced and their supply lines. This is followed by a generic brief on the components of IEDs, their types of firing switches and explosive theory followed up by a more detailed brief on the specific types of IEDs and their components relevant to the area of deployment. Understanding the electronic components of IED circuits should also be part of the training subjects taught so that WET can identify a type of firing circuit and the technology used even if they are recovering small pieces after a detonation.

Other subjects taught include how an IEDD team operate, how an IEDD task is conducted and what equipment is used, including how disposal procedures and the task can affect forensic evidence. Photography is also important as imagery will have to be collected of all aspects of the scene, the surrounding area and close up shots of the evidence recovered. Additional imagery includes being trained to draw sketch maps and plans to complement the imagery produced by photography. The forensic recovery taught covers biometrics, fingerprints, DNA, how tools by bomb makers leave marks and trace analysis. Questioning witnesses is also a required skill set which is different to the tactical questioning carried out on detainees by the force protection element of the responding force. The question techniques taught to WET are more in line with police procedures for interviewing witnesses but completed on the ground at the scene rather than at a police station. One of the most important skill sets that the WET need is the analysis of the overall attack and the ability to interpret the ground, technology used and method of attack. The team must understand why a particular piece of ground was used as the attack point, why a particular type of device was used, who the intended target was and whether this was as a result of security force vulnerabilities caused by incorrect TTPs or equipment. The attack must be then compared with previous attacks to identify patterns, trends and linkages. The next stage is to predict which TTPs the enemy will use in future attacks. All of this information must be put into a report that will need to be disseminated speedily and widely if a new enemy TTP is suspected or been discovered, the objective being to prevent further attacks by providing actionable intelligence to the targeting system or driving the development of force protection technology.

WET also train to attend sites that are being exploited through pre-planned search activities, including sensitive sites such bomb making factories,

known or suspected terrorist houses or caches of weapons and IEDs (whether components or complete). This also includes 'walk ins' where local nationals will remove IEDs and bring them to their local security forces, either for some form of reward or to remove the explosive hazard for safety or convenience reasons. If exploiting sites covertly that are not known to be compromised by the security forces, then WET need to be trained to carry out the insertion of tracking devices or replacing items such as explosives or weapons with inert items. As well as the core skills, WET are trained to operate all of their investigation equipment and force protection items such as electronic counter measures and night vision or thermal sights. If in a high threat environment then the WET will not only need thorough training on their personal weapons but also tactical shooting as individuals and as a team to be able to extract themselves from a contact. Other extraction training includes being able to extract their vehicle or themselves as individuals (including any wounded) from minefields if the WET are operating in areas known to be contaminated with mines.

Since WET investigations are normally conducted in post conflict countries and can be quite remote areas far from infrastructure, the team are likely to have to operate for longer in the field than planned and as such their training should include being able to sustain themselves in the field, environmental health training on local hazardous animals and plants and physical fitness (which should include carrying heavy rucksacks for distances on foot as the WET may be deployed by helicopter, and casualty evacuation). It should also include cultural training of the area they will be operating in and language training in the locally spoken languages (witnesses for interview may be local nationals, foreign soldiers or your own security forces). WET may not be deployed as a standalone team, but alongside a high risk search team and an EOD team. This reduces the amount of transport required for first responders and makes sustainment in the field easier for extended periods of time.

All WET reporting is combined with human intelligence reports from the interviewing of detainees and the exploitation of recovered electronic data to provide link analysis that drives further surveillance, arrest, search and targeting operations that seek to recover more evidence and detainees for further exploitation, which in turn drives more operations.

Once all the individual and team skills have been completed in the homeland then there is a requirement for pre-deployment training conducted in a realistic demanding environment that matches the area of operations. This means acclimatisation to different temperatures and operating conditions in a country that is the same as or very similar to the country of operations.

Throughout this training system, there needs to be a robust link with the operational theatre to ensure that all lessons identified during combat are rapidly passed back and integrated into future training. This can include instructors deploying to visit and study units in theatre and/or a second period of PDT in country whilst troops acclimatise.

We all know that the C-IED battle is a balance of technology, luck and most importantly training. Training has improved continuously and evolved in line with new equipment and the tactics of both ourselves and our adversaries. Training has proven itself to be the most cost effective way of saving life, and weapons exploitation training has proven itself to be essential in successfully defeating the IED networks. ■

ABOUT THE AUTHOR

Robert Shaw is a Security and Intelligence consultant. He retired from the British Army where he worked in the fields of IEDD and intelligence. Robert has managed training for the UN and NATO. Considered a C-IED SME, he has spent his career in a wide range of EOD, security and intelligence appointments that have ensured a global outlook. His experience includes Northern Ireland, Iraq, Afghanistan, the USA, Libya, Nigeria and Ukraine. Robert earned a master's degree in Global Security at Cranfield University and has three children.

POWERING THE THREAT: IMPROVISED BATTERIES FOR PORTABLE ANTI-AIRCRAFT MISSILES

By Lieutenant Colonel Jose M Rufas, Head of the Defeat the Device Branch,
C-IED Centre of Excellence

"Working for the power of the evil eye, we are never alone uncivilized."

(Bee Gees, extracted from the lyrics of the song "*High Civilization*", published in 1991 inside the equally named album)

After Cold War, the subsequent "small wars", and recent conflicts resulting from the so-called "Arab Spring", there is an impressive lack of control regarding the military depots from the fallen regimes or the governmental remains. Accordingly, and reinforced by the suspected and potential transfer from externally-supportive governments, there are huge amounts of Man Portable Air Defense (MANPAD) systems all around the world (but especially inside conflict areas, e.g. Libya), although they would be almost no use without operating batteries and other essential parts.

Model*	Country of manufacture	Quantity	% of total imports
SA-7b	Former Soviet Union	15,490	88%
SA-7b	Bulgaria	2,026	12%
SA-7b	Yugoslavia	22	<1%
Anza MK-II	Pakistan	4	<1%
SA-7b	Poland	4	<1%
Total		17,546	

Figure 1: Man Portable Air Defense (MANPAD) systems acquired by Libyan regime from 1973 to 1986.
(Source: http://www.smallarmssurvey.org/fileadmin/docs/G-Issue-briefs/SAS-SANA-IB2-Missing-Missiles.pdf)

Figure 2: "*Luftfaust*" model B (*Source: http://nnm.me/blogs/ss24k/wunderwaffe-tretego-reyha-pervyy-v-mire-pzrk/*) and "*Колос*" system *(Source: http://alternathistory.com/nemetskii-pzrk-lyuftfaust-vozdushnyi-kulak).*

Although initially designed for military use for defense at low altitude, the potential availability of shoulder-fired surface-to-air missile systems in the hands of threat networks is a persistent threat to not only military forces in the battlefield but also to fixed/rotary wing aerial vehicles in the homeland (e.g. areas surrounding airports).

Nevertheless, the ownership of that kind of anti-aircraft missile system is always hiding a huge dilemma for the potential user; he could have one of the single better tools to be able to terrify a whole country/organization/operation, but that mere possession is automatically transforming the owner into one of the most valuable targets for powerful actors all around the world… and any insurgency/terrorist group aspires to have other higher interests in benefit of his final intents rather than a single impressive action which is essentially hard to be successful.

With regards to consider, or not, a MANPAD with an improvised battery as an Improvised Explosive Device (IED), the definition[1] adopted by the North Atlantic Treaty Organization is wide enough to admit that kind of device under its domain.

WALKING DAVID AGAINST FLYING GOLIATH: A LITTLE BIT OF HISTORY ABOUT SOVIET MANPADs

Derived from the concept of the simple and effective anti-tank weapon known as "*Panzerfaust*", the *"Luftfaust/Fliegerfaust"* [2], an unguided multi-barreled (four or nine 20 mm barrels, or five 30 mm ones, depending on the different versions) rocket launcher, was developed by Germany in 1944; although the weapon was never mass-produced due to the end of World War II.

After World War II, Soviet designers also experimented with unguided multi-barreled rocket launchers "Колос" system, with seven 30 mm barrels), but this initially successful against helicopters/fixed wing airplanes design concept was abandoned in favor of guided missiles equipped with an infrared sensor, especially when United States started with the development of the FIM-43 "Redeye" system (precursor of the "Stinger") in late 50's.

The design of the first Soviet MANPAD was merely following Redeye's one, and it suffered a lot of engineering problems, especially regarding the miniaturization of an infrared seeker device, and gyroscope. In that manner, the 9K32 "Strela-2" system (Russian: Стрела, "arrow"; NATO reporting name SA-7 "Grail") firstly entered service in 1968, five years behind schedule, due to choosing a simpler (and less effective) seeker concept than Redeye.

The first combat experiences quickly proved that the system was very far from ideal. Its small impact warhead (1.17 Kg TNT charge inside a pre-fragmented case) was designed for chase attack, directly affecting the aircraft engine, as based on the poor infrared seeker design. Even when fired within the strictly limited engagement envelope, the hit probability was low (0.19-0.25). Furthermore, it turned out that a hit did not necessarily mean a kill, but only damage. There were other factors limiting its combat effectiveness; it could only engage a target moving at an altitude of between 50-1,500 meters, at speeds below 220 m/s (790 km/h or 425 knots), and not maneuvering more than 3.5 G.

In September 1968, it was decided to develop an improved model called the 9K32M Strela-2M, whose trials were conducted quickly, being accepted into

NAME	SYSTEM	MISSLE	LAUNCHING TUBE	GRIP-STOCK	BATTERY
Strela-2 (SA-7)	9K32	9M32	9P54	9P53	9B17
Strela-2M (SA-7B)	9K32M	9M32M	9P54M	9P58	9B17

service in 1970, and replacing the 9K32 on production lines. The 9M32M missile had a modernized guidance system that added the capability of engaging targets head-on, but only when moving slower than 150 m/s (540 km/h or 290 knots). Practically, only slow transport aircraft and helicopters could be attacked from the front . Moreover, the tail-shot engagement performance was improved so a target could be moving up to 260 m/s (940 km/h or 505 knots), the engagement range raised to 4.2 km, and the target-altitude limits expanded to 50-2,300 m. Along with that, the grip-stock was improved, and the triggering/firing system was quicker and easier.

As first generation systems, both 9K32/9K32M systems relied on a thermally activated chemical battery, uncooled PbS (lead sulfide) infrared detector, spin-scan optical modulation, high background noise, increasing tracking error near target, vulnerability to flares, and single-shot kill probabilities between 0.19 and 0.53. Several copies from them were developed by China (HN-5A), Pakistan (Anza Mk I), Former Yugoslavia (Strela 2M/A, 2M2J Sava), Romania (CA-94, CA-94M), Egypt (Ayn al Saqr), and North Korea (Hwasung-Chong).

The thermal battery[3] consists of an electrolyte and two electrodes. Unlike a conventional battery, however, the electrolyte (molten salts) is in solid state at room temperature and the battery is inert until the electrolyte is melted by a pyrotechnic device situated between the electrodes. Upon activation, the battery generates heat as a byproduct of the chemical reaction, leading to

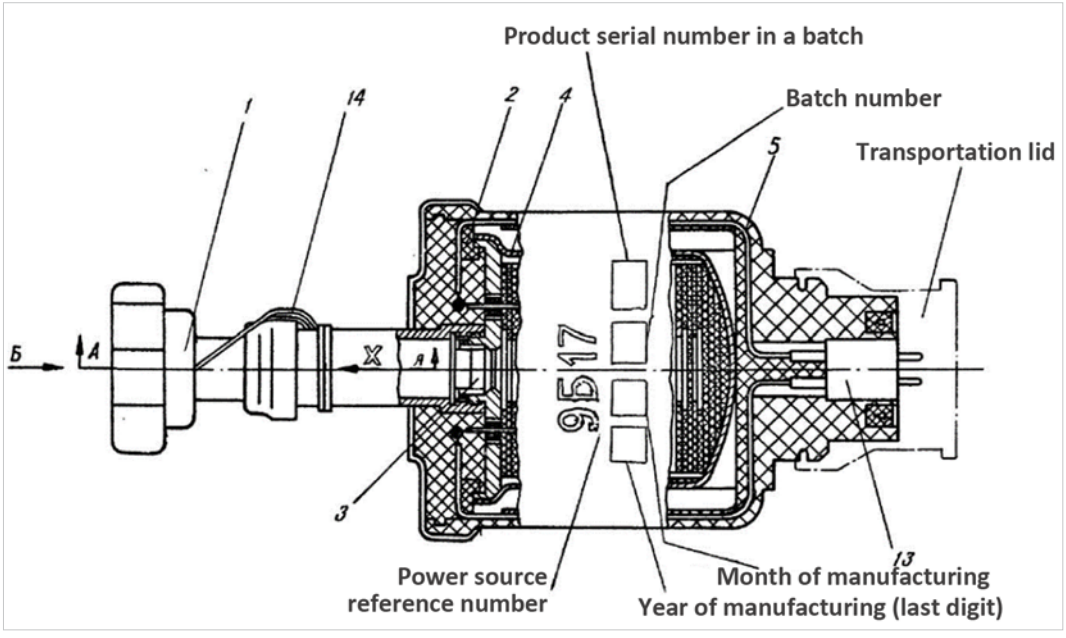


Figure 3: Technical cut scheme of the 9B17 battery from Strela-2/2M (SA-7/7B) MANPAD system, as drawn in the Soviet technical manuals for Strela-2M system.

temperatures of more than 200°C at the surface of the battery unit. The battery supplies power for gyroscope spin-up, the activation of the on-board thermal battery or generator, eject motor ignition, as well as some less energy extensive pre-launch processes. Due to its characteristics, the battery can be stored in solid state at room-temperature for long periods (when protected from moisture and oxygen, they can stay operational for 25 years and longer, although systems´ life used to be officially limited to 10- 20 years).

In the specific case of those first generation MANPADs, the battery is not including a cooling substance for the seeker, like next generations are, in which the "battery" is called the Battery Coolant Unit (BCU).

With regards to the Strela-2, the process for a good performance in firing the missile comprises: 1) spot the target and put launcher over shoulder; 2) turn the gunner percussion cap mechanism of the arrow printed on the battery end so the firing pin prick primer and the pyrotechnic mixture initiates(battery takes 5 seconds to start powering); 3) the gunner waits for electricity supply and gyros to stabilize, puts the sights on target and tracks it smoothly with the launch tube's iron sights; 4) once full power is ready, a sound from the grip-stock and a light signal in the sights informs the operator; 5) push trigger to half-position, which activates the seeker electronics and the missile attempts to lock onto the target; 6) when the missile is ready for launch, the target is producing a strong enough signal and the angular tracking rate is within acceptable launch parameters, another sound and light signal occurs; 7) if the target is outside acceptable parameters, then the light cue in the sight and the buzzer signal tells the gunner to re-aim the missile; 8) if everything is OK, the trigger is fully pushed, so the operator then has 0.8 seconds to provide lead to the target while the missile's on-board power supply is activated and the throw-out motor ignited; 9) the missile leaves the launcher. Each battery only has enough charge for 30-40 seconds, which sometimes might not be enough to complete a single engagement sequence!

The manufacturer lists reaction time measured from the carrying position (missile carried on a soldier's back with protective covers) to missile launch to be 13 seconds, a figure that is achievable but requires considerable training and skill in missile handling. With the launcher on the shoulder, covers removed and sights extended, reaction time from fire command to launch reduces to 6–10 seconds, depending greatly on the target difficulty and the shooter's skill.

In the case of Strela-2M (SA-7B), the grip-stock was slightly improved; accordingly, the new more automated grips-stock provided a simplified firing method against fast targets: a single trigger pull followed by lead and super-elevation replacing the separate stages of releasing the seeker to track, and launching the missile. The only problem was that the new version of grip-stock was not compatible with Strela-2, the previous model.

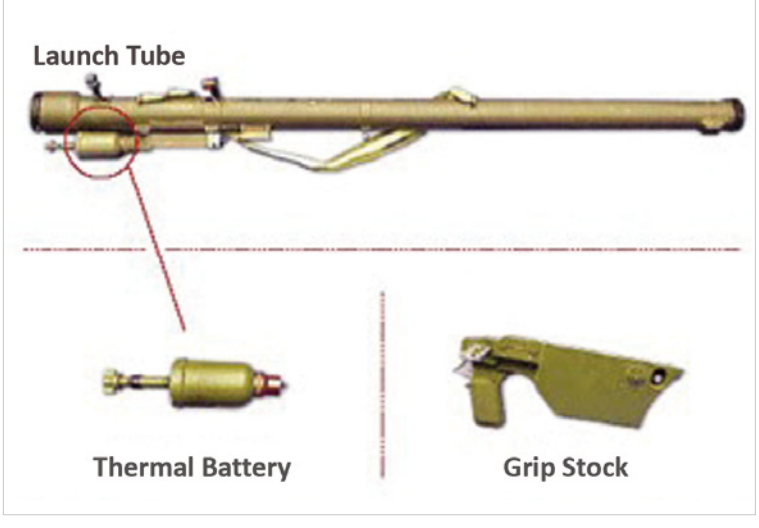


Figure 4: Essential components required to fire a first-generation MANPAD derived from Strela-2 series. *(Source: http://www.state.gov/t/pm/rls/rpt/walkearth/2008/105805.htm)*

IS THAT TERROR TOOL ABLE TO BE POWERED BY IMAGINATION?

Although several reports from national and multinational official sources are indicating that there are a lot of MANPAD systems uncontrolled and/or in the hands of potential terrorist groups or those able to provide them, they are practically harmless without batteries, and grip-stocks.

Initially, only first generation missiles could be potentially used with improvised batteries, due to next generations of MANPADs' need of cooling methods (mostly liquefied gases) for the seeker functioning along with the battery, which is almost impossible for homemade techniques (at least in a portable version).

Nevertheless, the Internet has been a "theatre" used to show several intents of designing and producing alternate power sources for SA-7 series/copied missile systems during recent years, as shown:

- (November 2012) Hamas al-Qassam Brigades – MANPAD is launched apparently using car batteries – missile detonates in the sky close to safety distance (https://youtu.be/B9nfqViBofk)
- (April 2013) Syrian Islamic Liberation Front – showing the design of 6 batteries for military equipment in series connected to missile system – without any evidence of practical functioning (https://youtu.be/Uic9bfUMgxg)
- (May 2013) Free Syrian Army FSA – MANPAD powered with an external battery (motorcycle one?) - **successful shooting against a helicopter** (https://youtu.be/aXGuUXbS3eo)
- (September 2013) "Al-Maghawir" (The Commandos) militias – video of MANPAD with external batteries shooting without apparent targeting success (https://youtu.be/lK15ggIWTYw)
- (October 2013) "Al-Maghawir" – showing effective

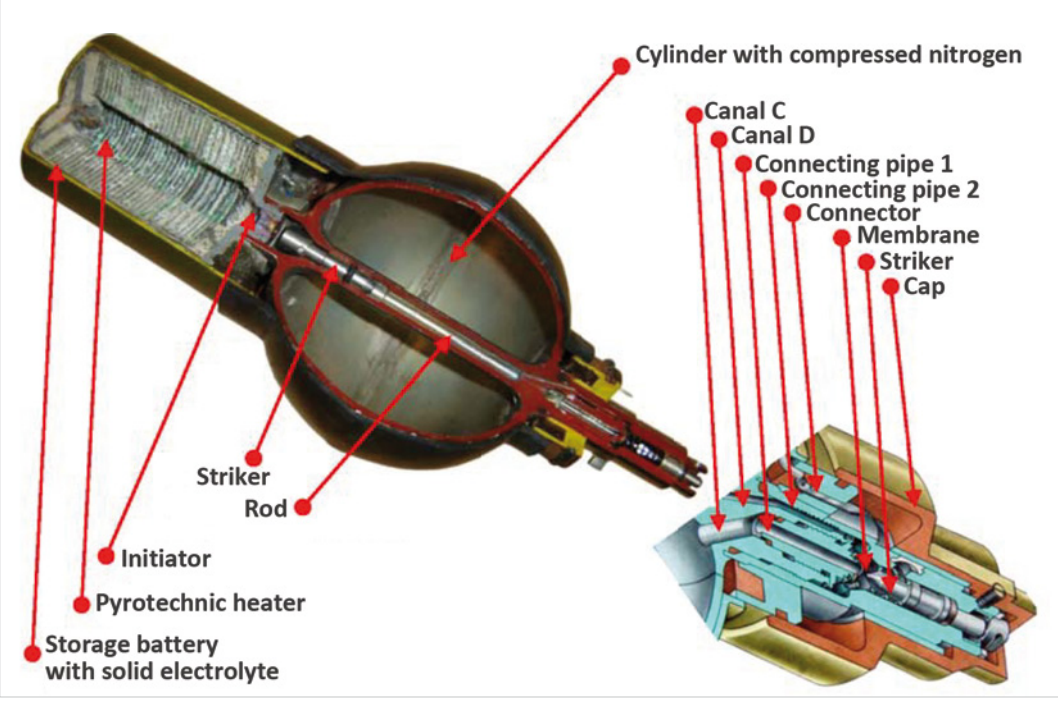


Figure 5: Cut scheme of the 9B238 Battery and Coolant Unit (BCU) for 9K38 "Igla" (SA-24) MANPAD.
(Source: ТЕХНИЧЕСКАЯ ПОДГОТОВКА КОМАНДИРА ВЗВОДА ПЗРК 9К38 «ИГЛА» (Platoon Commander Technical Training 9K38 MANPADS "IGLA"), Akylov/Baydakov/Vasiliev, 2011)

externally-powered MANPAD engagement over target and **success** (https://youtu.be/V-7Z3No7GzA)

- (April 2014) Jaysh al-Thuwar, 99th Infantry Brigade – a couple of videos in which an external battery (motorcycle?) system attached to a leg holster could be identified linked to the MANPAD through a wire – no evidence of practical functioning although they are quite similar to FSA's one shown before (https://youtu.be/bQPzhmG4pl4 & https://youtu.be/4yDYRaHEizQ)

Figure 6: Picture showing Ahrar al-Sham's improvised battery design in Syria.
(Source: http://armamentresearch.com/wp-content/uploads/2014/07/MANPADS_improvised.jpg)

- (June 2014) Ahrar al-Sham – highly portable improvised battery attached to 9B17 emplacement (similar to the one shown in figure 6) - the battery was good in firing the missile, which failed in flight (bad engagement of the target?); in accordance with the information received, the voltage dropped sharply once activated (https://www.youtube.com/watch?v=sA8nmUd2iFA)
- (July 2014) Free Syrian Army FSA – video shows Abu al-Baraa showing his design for a rechargeable battery made with 3 laptop ones plus a capacitor and some other electrical components recovered from electronic devices (http://nyti.ms/2hPmnW5)
- (July 2014) FSA - Facebook images showing a self-contained rechargeable battery pack. (http://armamentresearch.com/improvised-manpads-batteries-employed-in-syria/)
- (June 2015) Jaysh al-Yarmouk – external batteries (car ones?) – good launching but no target engagement (https://youtu.be/AHbO_09AKmI)
- (July 2015) Jaysh al-Yarmouk – MANPAD powered by external batteries (same as previous one) – it looks like a **successful impact** over a helicopter, although it is not fully clear (https://youtu.be/_enYMQh2y1Q)
- (January 2016) Video showing a Da'esh training school in which it looks like a design of a thermal battery for MANPADs has been successfully developed (https://youtu.be/A9tlDIhpMHo?t=298)
- (October 2016) FSA 46th Infantry Division – picture showing the shooting of a MANPAD powered by car batteries – effective shooting was reported although it failed due to target countermeasures – unconfirmed (https://now.mmedia.me/lb/en/NewsReports/567418-daraa-rebels-deny-receiving-anti-aircraft-weapons)

"IMPROVIDUS, APTO, QUOD VICTUM[4]"; HOW REALISTIC COULD THE REFERRED THREAT BE?

In accordance with the information shown above , merely a minority of the attempts were successful against slow aerial platforms like helicopters, all of them using power apparently from external batteries for vehicles… and everybody could understand that every successful targeting with a MANPAD is always something to make public knowledge in benefit of visibility and influence efforts; if there were any fully successful actions with those means, it would be quickly and widely publicized!

We should seriously consider that the potential use of improvised batteries powering MANPADs implies some big problems, not easy to solve or bypass;

- Need of appropriate grip-stock (different versions of missiles with specific required tools);
- Not very high rates of effectiveness, even against helicopters or transport airplanes;

- Limitations in directional attack, altitude, speed of target, vulnerability to countermeasures;
- Lack of adequate training (no good instructors, no previous shooting, no tactical training…);
- Evaluation of ageing missiles' functionality requires technical skills and knowledge;
- Bad storage conditions and no maintenance affecting all components of the systems;
- Sometimes, the energy would be only enough for propellant charge but not to power seeker;
- The use of car batteries transforms the MANPAD system to being effectively non-man-portable;
- Although possible, the design and manufacture of homemade thermal batteries is a hard task;
- In most of cases, the manufacturer has no accurate knowledge about battery requirements.

After analyzing the information collected from the Internet and once watching the videos, the real targeting success is not always as clear as declared (they celebrated the expected destruction/damage of the aerial vehicle due to missile effect, but it could be just the detonation resulting from the self-destruction of the warhead…).

Even the supposed ¨thermal battery design from Da'esh" could be a misunderstanding of some kind of manipulation over a thermal battery recovered from the body of another missile (info is partially given).

In conclusion, the threat regarding the use of 1st generation MANPADs with improvised batteries against commercial airplanes and helicopters is to a degree realistic; although it is not easy at all to achieve a good design and manufacture of the power source, but mainly to obtain good results with "jerry-rigged" batteries powering old missile systems with inadequate storage and maintenance… we will see! ■

"Where there is no imagination there is no horror."
(Arthur Conan Doyle, as written in his book "*A Study in Scarlet*", published in 1887)

Disclaimer

This article does not represent the point of view of any national or multinational organization. Its content should only be considered as the author's opinion.

REFERENCES

1 "A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores, but is normally devised from non-military components." (AAP-6 "NATO Glossary of Terms & Definitions", AJP-3.15 "NATO Doctrine for Countering Improvised Explosive Devices")
2 "Flying Fist/Air Fist"
3 Based on the "Thermally activated ("thermal") battery technology" series of articles written by R. A. Guidotti and P. Masset, and published in "Journal of Power Sources" Vol. 161-164-177-178-183, from June 2006 to April 2008.
4 (Latin quote) Improvise, adapt, overcome.

BIBLIOGRAPHY

- "Thermally activated ("thermal") battery technology" series of articles written by R. A. Guidotti and P. Masset, and published in "Journal of Power Sources" Vol. 161-164-177-178-183, from June 2006 to April 2008.
- Переносный зенитный ракетный комплекс "Стрела-2М" (9К32М) / Техническое описание и инструкция по эксплуатации (9К32М ТО), 1972
- ТЕХНИЧЕСКАЯ ПОДГОТОВКА КОМАНДИРА ВЗВОДА ПЗРК 9К38 «ИГЛА», Akylov/Baydakov/Vasiliev, 2011
- Наставление войскам ПВО - ПЗРК Стрела-2, 1969
- http://armamentresearch.com/improvised-manpads-batteries-employed-in-syria/
- https://www.nytimes.com/2014/07/26/world/middleeast/a-syrian-rebel-advance-off-the-battlefield-a-longer-lasting-rechargeable-battery-for-the-sa-7b-a-shoulder-fired-missile-system.html?_r=0
- https://www.bicc.de/uploads/tx_bicctools/BICC_brief_02.pdf

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. 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), Republic of Ecuador, Iraq and Uganda. ***Email: jrufas@ciedcoe.org***

CALL FOR PAPERS
COUNTER-IED REPORT

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

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

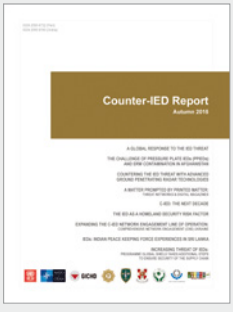
All enquiries and articles should be submitted by email to: editorial@deltabusinessmedia.com

For more information please visit: http://counteriedreport.co.uk/editorial

COUNTER-IED REPORT

Unique content I Global reach I In print and online

PRINT EDITION



WEBSITE

NEWSLETTER

eBOOK AND PDF

DISTRIBUTION AT THE EVENTS

Keep up-to-date with the latest C-IED, EOD and CBRNe news and developments.
Subscribe at http://counteriedreport.co.uk/subscribe