# OPPORTUNITIES FOR C-IED[1] CONCEPTUAL EVOLUTION IN LINE WITH EMERGING THREATS

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

> *"That was when I learned that words are no good; that words don't ever fit even what they are trying to say at."*
> (Willian Faulkner in his book "As I Lay Dying" first published in 1930)

We could find what English dictionaries are saying about "*improvise*"; "*to make or do something using whatever is available, usually because you do not have what you really need*" (Oxford Dictionary), "*If you improvise, you make or do something using whatever you have or without having planned it in advance.*" (Collins Dictionary), "*to make or fabricate out of what is conveniently on hand*" (Merriam Webster)…

The North Atlantic Treaty Organization (NATO) is officially defining an improvised explosive device (IED) as "*a device <u>placed or fabricated in an improvised manner</u> incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. (Note: It may incorporate military stores, but is normally devised from non-military components.)*".

On the other hand, United States Armed Forces are defining an IED as "*An improvised explosive device (IED) is a weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to kill, destroy, incapacitate, harass, deny mobility, or distract*". Although maybe not too much updated, even this basic definition is not well understood by many self-appointed C-IED experts without enough time for reading, and/or for trying to understand what they could read. That definition is wider than expected, by including conventional military munitions whose fuzes have been manipulated to arm them by aligning the fire train (e.g. what a VOG-17 series grenade needs to be ready to detonate when dropped by a drone).

If considering that the "IED" concept could cause confusion, try to understand what "C-IED" is: "*The collective efforts to defeat the IED system by attacking the networks, defeating the device, and preparing a force.*"…

Additionally, the term "C-IED" is often understood as not in line with NATO doctrine, so C-IED is widely understood in a wrong or limited manner:

- With a Defeat the Device (DtD) based on a reactive approach, mostly based on:
  - Military Engineer Enablers
  - Explosive Ordnance Disposal (EOD)
  - Military Working Dogs (MWD)
- And not including Attack the Networks (AtN) approach…

[1] *Countering Improvised Explosive Devices.*

## *C-IED after the retreat from Afghanistan: Just facing an evolving threat with some sort of obsolete approach!*

It is repeatedly stated, something similar to "*the fight against threat networks has been effectively taken, yet without any C-IED approach…*" by most of the C-IED detractors and/or those without any other knowledge on what C-IED could be other than the mere direct translation of the name into their local language.

Nevertheless, non-state actors have more or less successively defeated the West (and Russia) during the 20th and 21st centuries: just consider Afghanistan, Mali, Somalia, even Iraq… Why have we been unsuccessful if effectively employing intelligence and operations without applying Attack the Networks approach (so C-IED as it should be understood)?

Western countries have also failed in assuring an adequate training for host nations and regional coalitions regarding Attack the Networks, along with a real C-IED defence capability.

In fact, the latest NATO Strategic Concept 2022 is still considering non-state actors and terrorism as threats to fight against, as the following paragraphs are evidencing:

- *"… Terrorism, in all its forms and manifestations, is the most direct asymmetric threat to the security of our citizens and to international peace and prosperity. Terrorist organisations seek to attack or inspire attacks against Allies. They have expanded their networks, enhanced their capabilities and invested in new technologies to improve their reach and lethality. Non-state armed groups, including transnational terrorist networks and state supported actors, continue to exploit conflict and weak governance to recruit, mobilise and expand their foothold…"*
- *"… We will invest in our ability to prepare for, deter, and defend against the coercive use of political, economic, energy, information and other hybrid tactics by states and non-state actors…"*
- *"… Terrorist organisations threaten the security of our populations, forces and territory. We will continue to counter, deter, defend and respond to threats and challenges posed by terrorist groups, based on a combination of prevention, protection and denial measures..."*

Latest conflicts in Ukraine, Syria, Yemen… are not only posing a clear example of a hybrid threat environment in which powerful external state actors (e.g. the United States, Russia, Iran… along with their associated coalitions and proxy forces) are directly confronting their conflicting interests, and indirectly fighting between them inside the territory of another nation. The threat is suffering some evolving changes as follows:

- Both non-state actors and nations/coalitions are simultaneously facilitating, manufacturing, and using improvised explosive devices.

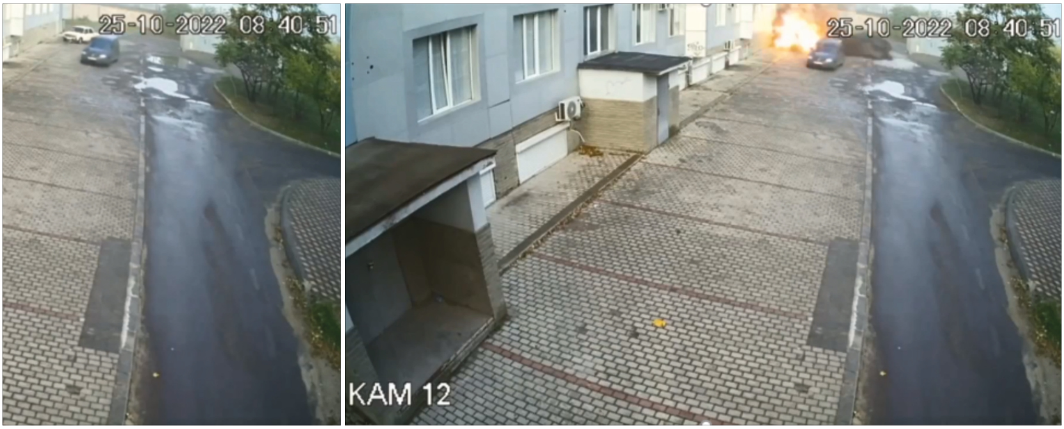
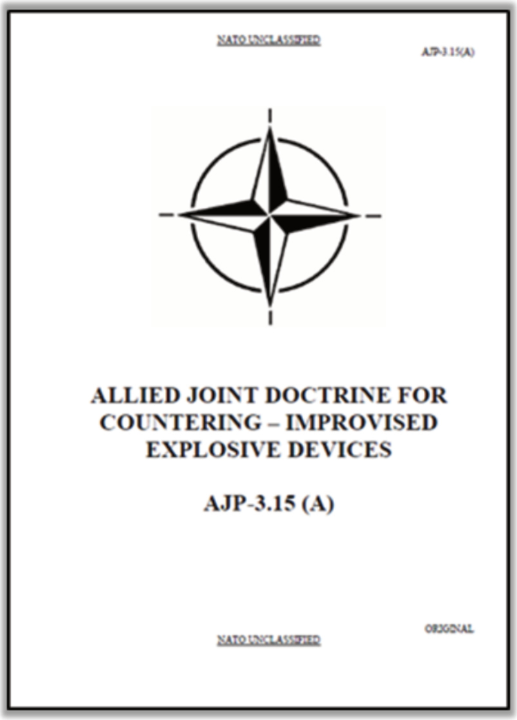


Figure 1: Detonation of a vehicle borne IED against a TV station in Melitopol, Ukraine, 25 October 2022. *(Source – Telegram)*

- Both non-state actors and nations/coalitions are employing improvised tactics, techniques and procedures (TTPs) with conventional and homemade devices and components.
- Both non-state actors and nations/coalitions are simultaneously facilitating, manufacturing, and using improvised weapon systems.
- Both non-state actors and nations/coalitions are simultaneously supporting and providing training in the use of the IED, improvised TTPs, and improvised weapon systems.

So effectively not only the ways and means, but the actors behind the improvised threat are different nowadays.

The change in the NATO approach to operations (less use of combat forces, and more supportive and training activity to a host nation) is causing a lack of "*boots on the ground*", direct collection of information, access to technical exploitation outputs, production of own intelligence, involvement in engagement and targeting… which is finally moving to a radical reduction in Attack the Networks capabilities.



NATO UNCLASSIFIED

AJP-3.15(A)

ALLIED JOINT DOCTRINE FOR COUNTERING – IMPROVISED EXPLOSIVE DEVICES

AJP-3.15 (A)

ORIGINAL

NATO UNCLASSIFIED

Figure 2: Cover of AJP-3.15(A) "Allied Joint Doctrine for Countering Improvised Explosive Devices", 2008.

*(Source – NATO)*

The threat is quickly evolving but the NATO C-IED approach has not changed from 2008… so what?

## *Same concept, different perspectives, and maybe a bit of massive confusion…*

The relative lack of success of NATO/United Nations/ Coalitions in recent operations against non-state actors, the reluctance to deploying troops for tasks other than training and advisory, and the change of geopolitical direction by the most relevant member countries of the Alliance could have guided (among other circumstances) a redirection of the focus of interest of the Alliance and its members.

Accordingly, the realistic estimate about a potential threat derived from the use of IEDs, along with the associated threat from non-State actors/Threat Networks affecting NATO territory and/or in allied operations seems to be currently underestimated.

All those referenced factors are contributing to create an intellectual environment open to wrongly consider C-IED as no longer an essential discipline for NATO.

Maybe it would not be a good indicator of a secure future for NATO capabilities in facing the improvised threat derived from unconventional adversaries that:

- NATO Headquarters International Military Staff (IMS) decided to cancel two internal C-IED-dedicated posts in 2013.
- Allied Command Operations (ACO) removed the unique dedicated internal C-IED post in 2018.
- Allied Command Transformation (ACT) decide to eliminate the C-IED Integrated Product Team (IPT) in 2016.
- NATO Operational Headquarters have dismantled the C-IED Working Group, and their dedicated C-IED elements are currently mainly focused on Force Protection (so merely DtD and PtF) but not always effectively considering the Attack the Networks (AtN) approach.

- NATO Tactical Headquarters are mostly embedding C-IED into Military Engineering, which is denying C-IED to have any AtN approach at all.
- Joint Warfare Centre (JWC), and Joint Forces Training Centre (JFTC) are lacking C-IED specialist posts inside their structure, which continuously causes them to request external support for allied exercises and other training activities.
- Joint Lessons Learned Allied Centre (JALLC) has no specific C-IED specialist posts inside their structure, which causes them to request external support from subject matter experts for analysis and lessons learned process's development.

United Nations (UN) is not considering Attack the Networks or an equivalent pillar inside their "Improvised Explosive Devices Threat Mitigation" approach: for UN, only Defeat the Device (DtD) and Prepare the Force (PtF) are considered inside the C-IED concept.

Accordingly, International Mine Action Standards (IMAS 04.10, updated February 2019) considered that *"C-IED is a government process specifically designed to reduce or eliminate the threat posed by improvised explosive devices. It is generally framed around three pillars of activity: attacking the network; defeating the device; preparing the force. Whilst prepare the force and defeat the device may relate to humanitarian mine action, attack the network does not as this would compromise the neutrality of the Humanitarian Mine Action community. As such, C-IED cannot be considered Mine Action."*

The European Union, through its European External Action Service (EEAS) developed their "*Concept for Countering Improvised Explosive Devices (C-IEDs) in EU-led military operations*" in 2016: then Attack the Networks was considered as a combination of Intelligence support by Troop Contributing Nations (TCNs), and Technical Exploitation.

Nonetheless, no effective "Attack the Networks" is conducted by the European Union, due to internal restrictions/limitations in Intelligence and Targeting/Engagement of EU-led operations. Intelligence is limited to Tactics,Techniques, Procedures as provided by member nations.

In fact, all C-IED projects developed by the European Defence Agency (EDA) are based on Improvised Explosive Device (IED) Awareness and C-IED Enablers (Military Search, Technical Exploitation, Route Clearance, Improvised Explosive Device Disposal IEDD…).

With regards to the "Five Eyes Only" multinational community, emerging GBR, USA, AUS, CAN & NZL[2] thinking is considering the term "'Non-Conventional Threat' (NCT)'' as a term that would sit above "IED"/ "C-IED" to allow similar strategies and capabilities, less DtD, to be conceptually applied to integrate other emerging threats and different physical threat vectors.

As the AtN, PtF and DtD type model can be applied to most threat vectors (IED, Chemical-Biological-Radiological CBR, Man-Portable-Air-Defense-Systems

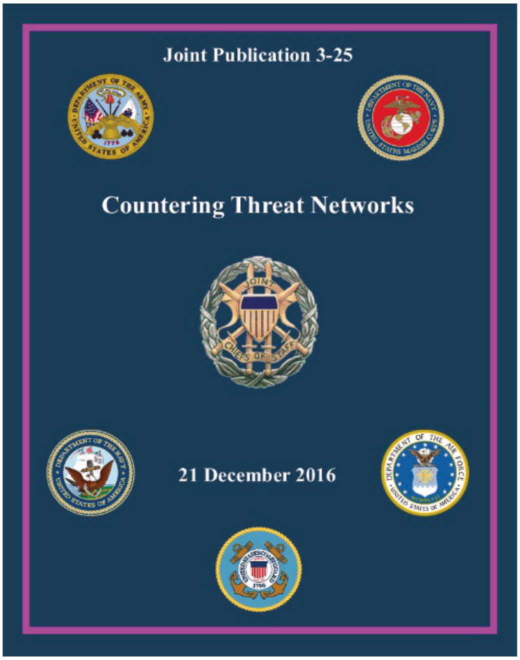


Figure 3: Cover of Joint Publication JP 3-25 "Countering Threat Networks", 2016. *(Source – www.fas.org)*

[2] *United Kingdom, United States of America, Australia, Canada, and New Zealand.*

MANPADS, Indirect Fire IDF, Small Unmanned Aircraft Systems UAS…), and Threat Networks are likely to be using multiple threat capabilities to achieve their objectives, a wider approach to counter the potential threat from non-state networks would be highly recommended.

United States Armed Forces are currently considering two different and separate concepts in line with NATO understanding for C-IED at Joint level:

- JP-3.25 "COUNTERING THREAT NETWORKS" (December 2016), which is described as the joint doctrine for joint force commanders and their staffs to plan, execute, and assess operations to identify, neutralize, disrupt, or destroy threat networks (so same as "Attack the Networks").
- JP-3.15.1 "COUNTERING IMPROVISED EXPLOSIVE DEVICES ACTIVITIES" (July 2018), which does not address Countering Threat Networks.

Nonetheless, and although the USA considers the AJP-3.15(C) approach for Allied operations, the Department of Defence (DoD) Counter-Improvised Explosive Devices (C-IED) and Counter-small Unmanned Aerial Systems (sUAS) portfolios have been transitioned from the Defence Threat Reduction Agency (DTRA) to the U.S. Army. DTRA retains Countering Threat Networks under its direction.

It currently looks like the USA is not going to persist with the "Improvised Threat" (although not an approved joint concept, it was defined as a compendium of improvised weapons, modified systems and ad-hoc tactics, techniques, and procedures - TTPs) approach, but consider "Weapons of Mass Destruction and Emerging Threats" instead.

In line with the previous statement, DTRA identifies the fight against weapons of mass destruction and improvised threat networks as a strategic goal.

US Armed Forces' Services (US Army, US Marines…) have adopted the "Network Engagement" concept as a tactical/component approach to Attack the Networks since 2017.

The current and likely future circumstances are strongly recommending a certain degree of evolution of the "C-IED" concept in the Alliance in logical adaption to face the evolving threats (as estimated in current/incoming scenarios), with the ability to frame the evolution of national lines of action.

In the short term, it is recommended to assess, promote and/or facilitate the development of some changes to the "C-IED" concept as follows:

- Maintaining the core spirit of former "C-IED" through not strongly modifying the aim, scope and functions, although accepting any evolution and modification.
- Making that evolution of the "C-IED" concept flexible enough to embed the potential answers to evolving and incoming threats derived from non-state actors and/or scenarios.
- Highly increase the relevance of countering those "Networks" (non-State actors or an equivalent evolving concept behind the potential threat to the interests of the Alliance and its member nations) in comparison with the more traditional focus in countering the "Device" (which is highly reactive and not adaptive, through limiting the scope and potentials of the concept).

## *Adhuc sub judice lis est*[3]*: opportunities for development are still open*

Aiming to adapt to the current and incoming threat environment, and the associated requirements to face it, the NATO C-IED concept should evolve:

- From a "device-centric" approach to a "threat-centric" one.
- From facing "improvised explosive devices" to face "the threat derived from improvised explosive devices, improvised weapon systems, and improvised tactics, techniques, and procedures".
- From a focus in "defeating the device itself" to one focused in "defeating those human networks behind the use of IEDs".

[3] (Latin language) "*The affair is not yet decided*".

- From mostly "reaction against the threat" to "anticipation to threat and reduction of the intended effects from those actors behind the threat itself".

In that way, C-IED should be focused in defeating some sort of "*unconventional threat*" or "*improvised threat*" defined in a similar manner as follows:

- "*Threat derived from the potential, effective or remnant use of improvised explosive devices or improvised weapon systems through the use of improvised tactics, techniques, and procedures (TTPs) by non-state actors (terrorists, insurgency, criminal organizations, proxy forces or any other violent extremist organization VEO), even promoted or indirectly utilized by state actors.* "

Accordingly, a new definition for "*Countering Improvised Explosive Devices* (C-IED)" or more preferably "*Countering Unconventional Threats* (CUT)" even "*Countering Improvised Threats* (CIT)" could be something such as:

- *"All joint and combined efforts in the aim of the reduction of potential effects derived from unconventional (or improvised) threats by means of integration, coordination, and synchronization of activities as conducted by allied forces, command structures, and interagency cooperation."*

So the C-IED/CUT/CIT… approach would be more or less based on:

- *"Integrate, coordinate, and synchronize all different staff and forces' efforts in planning and execution at all levels, which contribute to the reduction of the potential impact of the unconventional (or improvised) threat, with specific focus on engaging the actors behind it, and their capabilities."*
- *"For that there are key requirements: anticipatory focus, proactive posture, holistic considerations, interagency cooperation, and technical support."*
- *"The effective knowledge about the threat, and the actors associated to it, would require essential support from the outcomes of technical exploitation and human network analysis and support to targeting (HNAT)."*

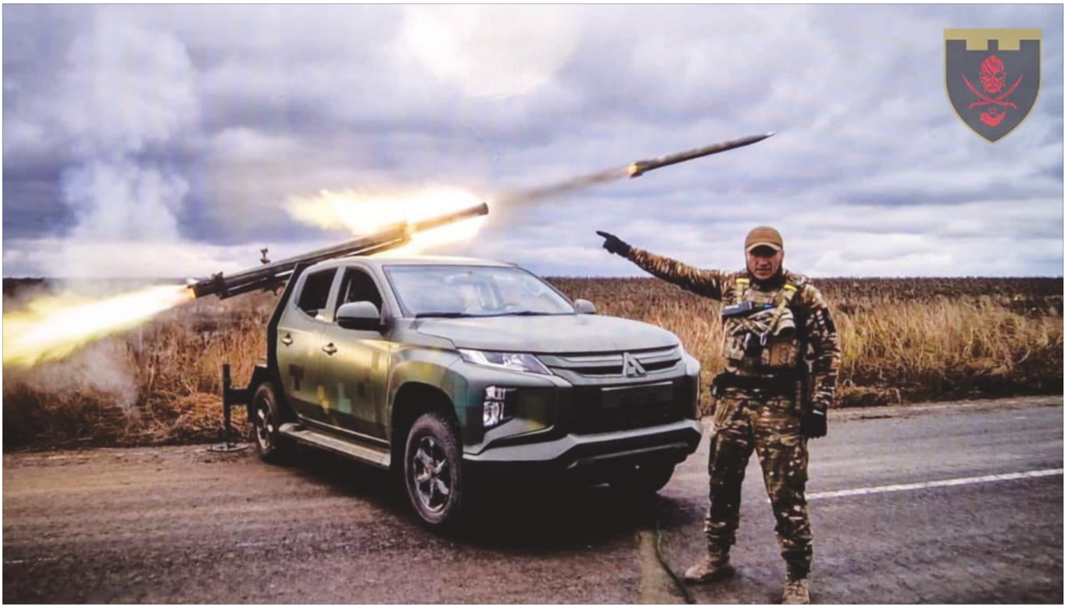


Figure 4: Improvised rocket launcher over a pick-up vehicle in Ukraine. *(Source – Telegram)*

## *Never trust anyone who has not brought a book with them!*[4]

The “C-IED” approach is currently under a real risk of being wrongly understood as not useful anymore for Alliance and the nations outside “Defeat the Device” and “Prepare the Force” pillars, and even to be substituted by another concept more adapted to the emerging threats. It would affect the functioning of current and future C-IED-related bodies, along with their concept, relevance, necessity…

From an analytical-synthetic perspective, it could be recommended - a potential evolution from “*Countering Improvised Explosive Devices* (C-IED)” into “*Countering Unconventional Threats*” (CUT) or “*Countering Improvised Threats* (CIT)”, due to it being considered the most adaptive, balanced, flexible, progressive, and viable option to be potentially accepted by member nations.

As the AJP-3.15 “Allied Joint Doctrine for Countering Improvised Explosive Devices (C-IED)” is currently under review process, it could be a nice opportunity for a smart evolution and adaption to the existing and incoming threat environment. ■

> *“Yesterday's dangerous idea is today's orthodoxy and tomorrow's cliché.”*
>
> (Attributed to Richard Dawkins by John Brockman, in his book "What Is Your Dangerous Idea?: Today's Leading Thinkers on the Unthinkable" first published in 2009)

## Disclaimer

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

## ABOUT THE AUTHOR

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

***E-mail: jrufas@ciedcoe.org***

[4] From “*Horseradish*” by Lemony Snicket.