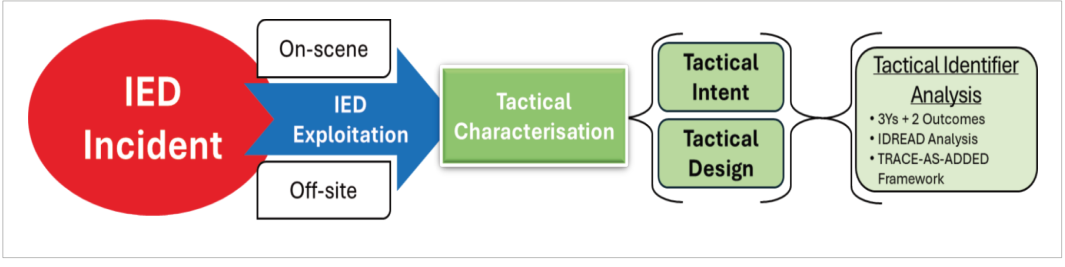
# INSIGHTS INTO IED EMPLOYMENT
## IED TACTICAL DESIGN PROFILES AND SIGNATURES

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

### INTRODUCTION

Continuing our 5W+H series on IED attacks, intended to provide a comprehensive understanding of the use and threatened use of IEDs, having previously explored their technical aspects,[1] this article continues our examination of how these devices are employed. The previous article in this series, examined how IEDs are employed through the use of tactical identifiers allowing classification by tactical employment and by tactical characterisation. Tactical characterisation of IED attacks involves assessing their tactical intent and tactical design for which three means of analysis were presented: 3Ys and 2 Outcomes, IDREAD analysis and the TRACE-AS-ADDED[2] framework. Building on the foundation laid in Exploring IED Employment – Understanding the 'How' of IED Attacks,[3] this article examines how tactical design profiles and IED tactical signatures can be developed.

The next article in this series will explore how tactical design profiles can be integrated with other C-IED analysis products to produce IED incident profiles. Over time, when these profiles are subjected to pattern and trend analysis, they can be used to assess the tactical sophistication of the IED threat. Ultimately, evaluating the tactical sophistication of the IED threat




Process for the Tactical Characterisation of an IED Incident.

1 A Journey Through PIECES of SPICE PIES, The Counter-IED Report, Spring-Summer 2025.
2 Acronym for, Tactical intent; Role; Attack geography; Conditions when found; Environmental conditions; Atmospherics; Sensor defeat; Attachment method; Delivery; Domain; Employment method; and Discovery method.
3 Exploring IED employment – understanding the 'how' of IED attacks, The Counter-IED Report, Spring/Summer 2025.

informs the design, development, and continuous refinement of an accurate threat picture.[4] We begin by examining the need to strike a balance between recognising the tactical uniqueness of individual IED incidents, identifying evolving commonalities through pattern recognition, and detecting inevitable changes in IED tactical employment over time.

## FINDING THE RIGHT BALANCE - TACTICAL DESIGN PROFILES, SIGNATURES, AND THE EVOLVING IED THREAT

Effectively assessing and communicating the tactical sophistication of an IED threat involves using tactical design profiles for individual incidents and tactical signatures for clusters of incidents that share commonalities in tactics[5] employed. This process requires an understanding of the improvised and adaptable nature of these attacks. IED attacks do not follow fixed templates. Instead, they reflect context-specific nuances shaped by the type of IED being employed, the tactical intent behind its use, and the environmental factors present at the attack location.

Attempts to impose rigid templates when analysing IED tactical employment risk overlooking key variations and the inherent nuances of how IEDs are used in individual attacks. Each incident is unique and context-specific, so the headings within a tactical design profile may vary to reflect the specific data that need to be captured. Despite these inevitable nuances, recurring patterns in IED employment often emerge over time, revealing commonalities across incidents within a given threat environment. Similar tactical patterns tend to arise when IED attackers pursue the same objectives within comparable environments. These shared conditions constrain available options and promote the use of proven methods, resulting in recurring tactics across incidents. Tactical signatures are used to capture and communicate these shared commonalities in IED tactical employment across multiple attacks.

Once such commonalities in IED employment are identified, efforts can be invested to counter the tactics identified. This, in turn, typically forces the IED system to change the technical complexity of their devices and the tactical sophistication of their attacks. This dynamic plays out as a “cat and mouse” interaction, more formally described as an action–reaction–counteraction cycle, between IED attackers and the C-IED community.

This inevitable evolution in the threat requires that changes be detected and tactical sophistication assessments updated through amended tactical signatures. Tactical signatures must therefore be updated regularly, tailored to the operating context, and supported by real-world examples when possible. They should also be managed under appropriate information security protocols and disseminated in a timely, targeted manner to those who need them most. Striking the right balance, between recognising the uniqueness of individual incidents, tracking evolving tactical commonalities across certain incidents, and monitoring trends over time to detect changes, is essential to understanding an IED threat’s tactical sophistication.

## TACTICAL DESIGN PROFILES

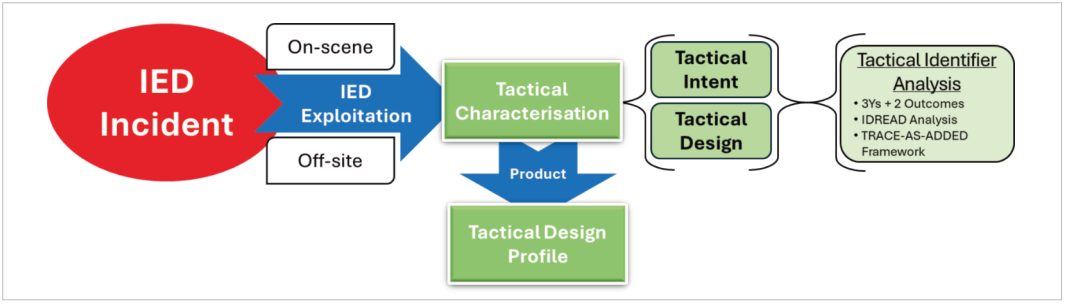
Tactical identifiers refer to the observable and inferable tactical features of how an IED attack is planned and executed. They describe how an attacker employed, or intended to employ, a device in relation to the target, within the context of the operational environment and local factors, to achieve the intended target effect. These identifiers are derived from analysing tactical factors such as delivery mechanism, placement, use of terrain, initiation method, coordination of attack cycle elements, and the concealment employed. Tactical design profiles can be developed using one or more of the three primary methods for tactical characterisation: the 3Ys and 2 Outcomes approach, IDREAD analysis, and the TRACE-AS-ADDED framework. They may be applied individually, in combination, or selectively.

4 An IED threat picture is an assessment of the use or threatened use of IEDs in terms of the technical complexity, tactical sophistication, the IED system employing them and local context. The IED system is assessed under its intent, capabilities and the opportunities it has to employ IEDs against defined target(s). Local context is defined by a geographic area, the target of the attacks and other local factors.

5 Carefully considered actions intended to achieve a specific aim.

| 3 Ys & 2 Outcomes | IDREAD Analysis | TRACE-AS-ADDED Framework |
|---|---|---|
| ***Why here?*** | **I**ntended purpose | **Tactical Intent**<br>**Role**<br>**Attack Geography**<br>• *Device placement characteristics*<br>• *Contact point characteristics*<br>• *Command IED specific considerations*<br>• *Post blast data*<br>**Conditions when found**<br>**Environmental conditions**<br>**Atmospherics**<br>**Sensor Defeat**<br>**Attachment method**<br>**Delivery**<br>**Domain**<br>**Employment Method**<br>**Discovery Method** |
| ***Why now?*** | **D**elivery method | |
| ***Why in this way?*** | **R**ole | |
| ***What was the intended outcome?*** | **E**mplacement location | |
| | **A**ttachment method | |
| ***What was the actual outcome?*** | **D**evice Orientation | |

Comparison of the three methods that can be adopted, adapted or combined to construct tactical design profiles.




A process by which tactical design profiles can be developed.

## IED TACTICAL SIGNATURES

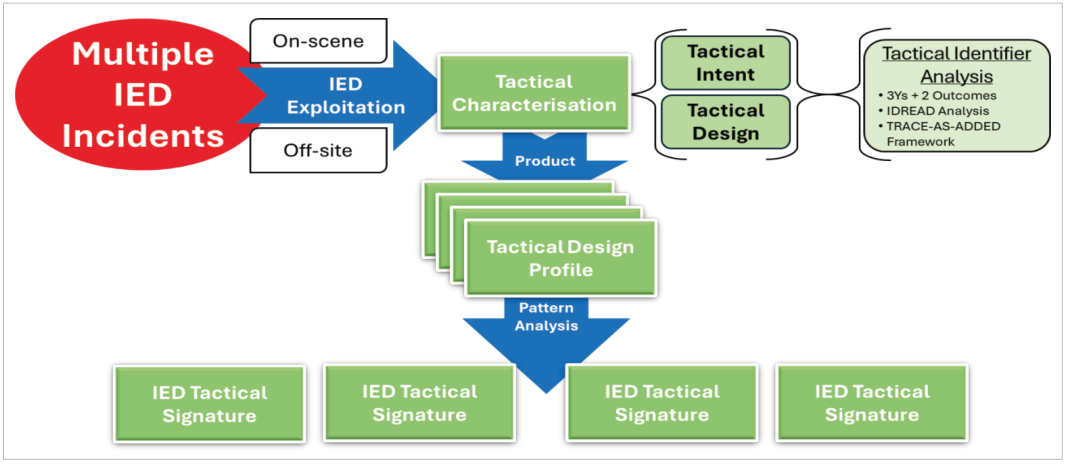
When tactical identifiers are consistently gathered on scene and analysed off site, and the resulting data is systematically compiled under standardised headings within tactical design profiles and entered into an appropriate Information and Knowledge Management (IKM) system, effective pattern and trend analysis becomes possible. Over time, structured analysis of IED tactical identifier data across multiple tactical design profiles enables the identification of recurring characteristics in IED deployment. These characteristics reveal how IEDs are planned, delivered/emplaced and executed in relation to varying operational contexts. The recurring tactical characteristics identified through this process inform the development of informal, yet often insightful, descriptive IED tactical signatures. IED tactical signatures are narrative tools that provide insights into specific objectives, modus operandi[6] and other tactical behaviours of networks within a given context. In contrast to the more systematic and formulaic tactical design profiles used for individual IED attacks, tactical

6 Method of operation; style of handling things. Source: St. Andrew's University, Certificate/Advanced Certificate in Terrorism Studies, Terrorism Glossary.

signatures offer a flexible and intuitive means of expressing attacker intent and tactical behaviour across multiple incidents. By highlighting key tactical characteristics observed across incidents, tactical signatures present a contextual overview of tactical designs tailored to specific objectives. When systematically developed and supported by practical examples, they serve as powerful communication tools within the C IED community.

These signatures provide a means of assessing the tactical sophistication of the IED threat. Once established, monitoring IED tactical signatures collectively over time through trend analysis helps reveal shifts in the threat, including escalation in violence and adaptations in response to countermeasures. Subsequent pattern analysis allows tactical sophistication assessments to be updated accordingly. This, in turn, supports timely amendments to the IED threat picture, ensuring it remains accurate and informative.

Together, pattern and trend analysis of tactical design profiles offer insights into attacker intent, capability and tactical sophistication, directly contributing to C-IED understanding and decision making. These analytical approaches support proactive threat mitigation and preventative operations. The examples provided below illustrate how IED tactical signatures can be developed to reflect specific operational contexts and threat environments. These signatures aim to convey how IEDs may be employed tactically; however, it is emphasised that for a given threat environment, specific IED tactical signatures need to be developed and updated over time. It should be noted that some commonly cited IED tactics, such as secondary IEDs, suicide IEDs and proxy IEDs, are not included in this selection. In particular, secondary IEDs are considered more reflective of the IED role[7] within an attack, which has already been addressed as a tactical identifier.[8] In the case of suicide IEDs[9] they are not outlined here as a standalone tactic but are covered within the IED tactical signatures of SVBIED attacks on convoys as well as breaching using PBIED or SVBIED. Finally,




Process by which IED tactical signatures can be developed over time.

7 Designating an emplaced IED as a primary, secondary, or subsequent form of attack. Primary is used for an IED assessed as the most tactically significant IED within an incident while a secondary IED refers to any additional IED(s) used to attack individuals or vehicles after an initial event. Source: Adapted from, The IED Incident Reporting Guide, 6th Edition.

8 See Exploring IED Employment – Understanding the 'how' of IED attacks, The Counter-IED Report Autumn 2025.

9 In a previous article, the author set out the argument that suicide IEDs are a special category of command IEDs; however, acknowledged that in some systems they are considered a separate method of IED actuation. IED Classification – Breaking Down Bomb Attacks, The Counter-IED Report, Spring/Summer 2025.

proxy IEDs[10] have previously[11] been considered as a subset of suicide IEDs, which are themselves classified as a special type of command IED. However, this does not preclude the development of IED tactical signatures for secondary, suicide and proxy tactics when such employment is common in a given threat environment.

## Area Denial IEDs

This involves the use of IEDs in a similar manner to the employment of landmines and conventional boobytraps. Such IED tactics have been seen in Iraq and Syria as well as in Somalia. Typically, the main charge is buried close to a victim-operated switch and left unattended. Area denial IEDs may be designed for use against personnel or vehicles and may be placed singly along a canalised route or in multiples. They may also be emplaced in urban spaces, routes and approaches to known areas a target is likely to use and can often be indiscriminate in their targeting. Multiple devices may be laid to increase the probability of a strike, or they may be sited as secondary IEDs to attack personnel responding to an initial strike.

## Command IED Ambushes / Complex Attacks on Mobile Targets Possibly Using Spotters

Command IEDs can initiate an ambush or be deployed after an ambush has been triggered by other means, such as small arms or light weapons (SALW) fire. These are often referred to as complex attacks. Typically, a buried or concealed surface laid IED is placed[12] along a known route of travel of a vehicle convoy, patrol, or a target moving on foot. Such attacks may incorporate the use of spotters, depending on the line of sight from the firing point to the target's approach route to the contact point. Spotters are often positioned at elevated or concealed vantage points within the surrounding area, tasked with observing potential avenues of approach.[13] Depending on the type of IED being used, the spotter provides a signal to the triggerman to prepare to initiate the IED or remotely arm a VOIED. When the target reaches the contact point, the ambush is initiated. The goal is to kill or injure the target, damage vehicles, or render them immobile within the ambush's kill zone. More advanced tactics may aim to block the target's extraction or withdrawal route by targeting the lead and/or rear vehicle. Once trapped in the kill zone, the target may be further immobilised by secondary anti-vehicle or anti-personnel IEDs placed in the surrounding area. SALW are then often used to attack the fixed target within the kill zone.

## Come-on / Lure IEDs

An attacker may draw a target into close proximity of the lethal radius of an IED by attracting their attention or arousing their curiosity by placing a valuable, attractive, familiar or tactically important object near the IED. Trophies such as flags, and other items of interest to the intended victim are left to be seen and picked up but are boobytrapped with a victim operated firing switch. Familiar items of equipment such as rifle magazines, radio batteries, torches and water bottles often do not arouse suspicion because they look as though they were dropped, and it is natural to recover them. In more sophisticated come-on IED attacks, a conspicuous IED, weapon system, or corpse is deliberately left in plain sight to lure security forces into a specific area for

10 When a suicide IED is delivered by an individual who has been coerced into carrying out the attack or is unknowingly transporting the device to its target, it is classified as involving a proxy bomber rather than a suicide bomber. The level of control and assurance of success with proxy bombers compared to suicide bombers is lower, as the person delivering the device may not act as directed, or if carrying the device unwittingly, may act in an unplanned manner. IED Classification – Breaking Down Bomb Attacks, The Counter-IED Report, Spring/Summer 2025.

11 In the previous article IED Classification – Breaking Down Bomb Attacks, The Counter-IED Report, Spring/Summer 2025, the author considered considering suicide IEDs involving either suicide bombers or proxy bombers, as a form of command IED; however, some systems consider suicide IEDs as a separate method of IED actuation.

12 Command IED ambushes are often referred to as complex attacks as they involve coordinated use of multiple tactics, such as combining small arms, IEDs, vehicle attacks, and suicide operations, often targeting both people and infrastructure. They require higher levels of planning, synchronisation, and resources. However, this term is also used and connected to marauding terrorist attacks. More information on this is provided in the IED tactical signature 'Breaching Using Person-Borne and Suicide Vehicle-Borne IEDs' below in this article.

13 Spotters may also be employed over time to monitor the behaviour of security forces, with the intent of exploiting observed patterns as part of TTP (tactics, techniques, and procedures) identification. Their role can include gathering intelligence to inform attack planning, understanding security force tactics, and directly assisting in the execution of IED attacks. Additionally, spotters may record attacks for messaging purposes or use the footage for training and the ongoing refinement of tactics through a lessons-learned process.

recovery. In such cases an unseen IED is emplaced to target the security forces. Such come-on incidents may involve information being provided to the security forces about the location of these items or placing them in a location where they are intended to be discovered. Finally, emplacing a VOIED or command IED at the firing point of an attack or the launch point of a standoff IED is another example of a come-on IED attack. In this case, the attacker knows security forces typically move to search and exploit such locations. Come-on IEDs can harass and significantly degrade confidence by instilling fear in security force members leading to hesitation in action resulting in a decrease in the tempo and progress of operational activities as operating in such threat environments needs to be done with extreme caution.

### Reoccupation IEDs / Boobytrapping

VOIEDs may be positioned at known security force locations to exploit the likelihood that these positions will be reoccupied in the near future. This tactic typically occurs in two ways:

- Predictable occupation patterns – Security force locations, such as observation posts, checkpoints, or stand-to positions, may only be manned during specific, often predictable times and left unattended at others.
- Post-overrun reoccupation – A security force position may be overrun, with the expectation that reinforcements will counterattack and reoccupy the site.

In both scenarios, concealed IEDs are emplaced to kill or injure security forces entering the area. This tactic is comparable to boobytrapping fighting positions in conventional warfare – designed to inflict casualties on attackers when such positions are abandoned or captured. The use of reoccupation IEDs can significantly undermine the confidence of security forces moving to occupy these locations.

### Coordinated IED Attacks - Multiple IED Attacks at a Given Time and Area

Attackers can orchestrate multiple IED incidents at different locations simultaneously, exploiting the limited resources of security forces. While security forces might manage to respond to several incidents in quick succession, handling multiple incidents at the same time poses a significant challenge. Coordinated IED attacks are highly disruptive, instilling fear among the local population and physically and psychologically straining the responding security forces. These attacks often combine real IEDs with hoax devices, which are easier to prepare and further complicate the security forces' response efforts.

### Hoax Incidents[14]

Hoax incidents involve incomplete devices or materials designed to resemble an IED. Their purpose is to provoke a security force response or instil fear in a target group, thereby deterring both security forces and the target group while gradually undermining morale. These incidents may also disrupt daily activities in the target location and challenge the legitimacy of governing authorities. Hoax incidents can function as part of broader coordinated IED attacks or constitute all the incidents in a coordinated series of disruptive events. Additionally, attackers may use hoaxes to monitor the actions of responding security forces as part of TTP identification. Hoaxes enable attackers to achieve objectives with minimal effort compared to constructing and emplacing real IEDs.

### Spoofing[15]

A variation of the hoax tactic, spoofing is designed to trigger a false positive indication of an IED by the search procedures or equipment being used. It may involve exploiting visual searches, working animals, or search-and-detection sensors, by falsely providing an

14 Hoax IED incidents are different from false IED incidents, which refer to an incident incorrectly identified, though reported in good faith, as an IED, which is subsequently categorised as a false alarm after positive EOD action. False IED incidents are sometimes referred to as false alarms.

15 Spoofing, when used as an IED tactic, differs from its application in electronic warfare, where deceptive signals are transmitted to mislead or manipulate targeted systems. For instance, fake signals may mimic legitimate ones, tricking the targeted receiver into accepting and acting upon false data. For example, GPS spoofing, a specific form of electronic warfare, involves sending counterfeit GPS signals to mislead navigation systems. Additionally, spoofing in electronic warfare can be employed to analyse the response of the targeted system, similar to TTP identification. These tactics are extensively used in drone and counter-drone warfare and are increasingly observed in the IED drone nexus.

indication of the presence of an IED component. It typically involves contaminating a location with items or materials that generate a false positive response from the search procedure or equipment in use. The goal is to provoke a response from security forces when a false positive is detected. This delays the search process, disrupts operational tempo, and gradually erodes confidence in procedures and equipment. Moreover, spoofing often leads security forces to repeatedly deploy countermeasures and equipment, which when combined with spotters, can support TTP identification.

### Trojan Horse IEDs

Trojan horse IEDs involve an IED delivered surreptitiously by someone unwittingly to a target. They are often hidden within items expected to be brought to the target location by authorised individuals. These items might hold forensic or intelligence value or be considered a memento or trophy. A parcel IED sent by mail or courier delivery service is a variation of a trojan horse IED tactic.

### Suicide Vehicle-Borne IED (SVBIED) Attacks on Convoys

SVBIEDs are used to strike convoys, patrols, or high-value targets in transit. Their mobility allows attackers to deliver large charges with precision by closing distance to the target, often bypassing fixed defences. This tactic merges manoeuvrability with lethality, enabling the attacker to guide the device directly to its objective while carrying a payload far greater than that of most static IEDs or Person-Borne IEDs (PBIEDs). Due to the complexity involved in planning, resourcing, and executing such attacks, SVBIEDs are typically considered high-value assets and are employed sparingly by well-organised networks.

### Breaching[16] Using Person-Borne and Suicide Vehicle-Borne IEDs

PBIED and SVBIED can be employed to breach the defences of secure locations. This is often the initial action that enables other attackers to enter the secure location as part of a complex attack or marauding terrorist attack.[17] Follow-up attackers exploiting the breach may include additional SVBIEDs, person-borne suicide bombers, or assault infantry equipped with SALW systems such as vehicle-mounted heavy machine guns, rifles, hand grenades, or self-propelled grenades.

### Messaging / Propaganda and Influencing

Key objectives of IED attacks often include instilling fear in a targeted group, undermining ruling authorities, and/or gaining the support of a segment of the local populace through a demonstration of power. All of these objectives typically involve elements of propaganda to convey the intended message. Some IED attacks may be symbolic, designed to send a message to specific groups and influence their perceptions or actions. Such messaging can involve issuing statements after an IED attack, sometimes accompanied by footage showing the preparation and execution phases. In certain cases, this material is highly professional and distributed through various channels. The advent of social media has dramatically amplified the reach and speed of such propaganda. Footage may include imagery captured by spotters, drones, or body-worn cameras.

16 Breaching is an example of a class of IED attack based on target effect. See IED Classification – Breaking Down Bomb Attacks, The Counter-IED Report, Spring /Summer 2025.

17 Complex attacks and marauding terrorist attacks (MTA) share many overlapping features, but they are not always synonymous but exist on a spectrum of coordinated violent tactics. MTA typically refers to "fast-moving, violent incidents where assailants move through a location aiming to find and kill or injure as many people as possible."[A] MTA can involve lone attackers or coordinated groups, and may include the use of firearms, bladed weapons, explosives, or a combination of these. The 2008 Mumbai attacks and 2015 Paris attacks are often cited as exemplars. Complex attacks, on the other hand, involve coordinated use of multiple tactics, such as combining small arms, IEDs, vehicle attacks, and suicide operations, often targeting both people and infrastructure. They require higher levels of planning, synchronisation, and resources. A MTA can be a component of a complex attack. For example, a complex attack might begin with an IED detonation to cause confusion or gain entry to a target, followed by marauding gunmen targeting fleeing civilians or first responders. In that sense, MTAs are often nested within complex attacks, or vice versa, depending on how an attack is designed. NOTE: Complex attack is also used at times to describe command IED ambushes.

Source: A. UK National Protective Security Authority, https://www.npsa.gov.uk/emergency-incident-management/marauding-terrorist-attacks

## Use of Drones in IED Attacks

Uncrewed Aerial Systems (UAS)[18] are a versatile tool in support of IED attacks. They can serve multiple roles, including intelligence, surveillance, reconnaissance, and target acquisition (ISTAR); functioning as platforms for delivering explosive ordnance; and enabling post-attack analysis for messaging or facilitate lessons learned. Their accessibility and adaptability have made them a favoured asset not only among state actors but also non-state armed groups and criminal organisations. As a result, the aerial domain has become more accessible and active, significantly reshaping IED threat environments.

Aerial drones may support IED attacks as an unarmed or armed enabler. For example, aerial drones may be used to surveil or reconnoitre a static location being targeted allowing intelligence to be gathered which can inform an attack plan. During an attack, aerial drones can monitor the target and assist in attack coordination. For example, a UAS can be used as an aerial observation platform for a coordinator in communication with a SVBIED or person-borne suicide bomber, to guide them toward breach points or to opportunistic targets as they emerge e.g. people fleeing an attack or security forces responding to an attack. The same aerial drone footage can subsequently be used for messaging and lessons learned purposes post attack. At the same time, armed aerial drones, to deliver items of explosive ordnance to a target have transformed the threat from a two-dimensional to a three-dimensional challenge. Traditional layered defences against IEDs now need to account for vertical threats, requiring protection not only around a target but also above and over it. For example, aerial drones can now be deployed as observation platforms using first-person view (FPV) capabilities and equipped with various explosive ordnance payloads. These payloads may be released inflight, functioning as improvised aerial bombs, or launched from the drone itself. Alternatively, the drone may be directed to crash into a target, a tactic commonly referred to as a kamikaze or one-way attack drone. This combination of observation followed by target acquisition and attack is akin to improvised loitering munitions. What was once the preserve of state and military actors has now devolved to the tactical battlefield and accessible to non-state actors and even criminal groups operating in contested spaces. As such one might speak of a revolution in military affairs[19] – but this time it is an improvised revolution.[20] Owing to the nexus between the dual use nature of many of the UAS used and the readily available know-how on the internet, pandora's box is now open and cannot be closed to the use of aerial drones to support IED attacks.

## CONCLUSION

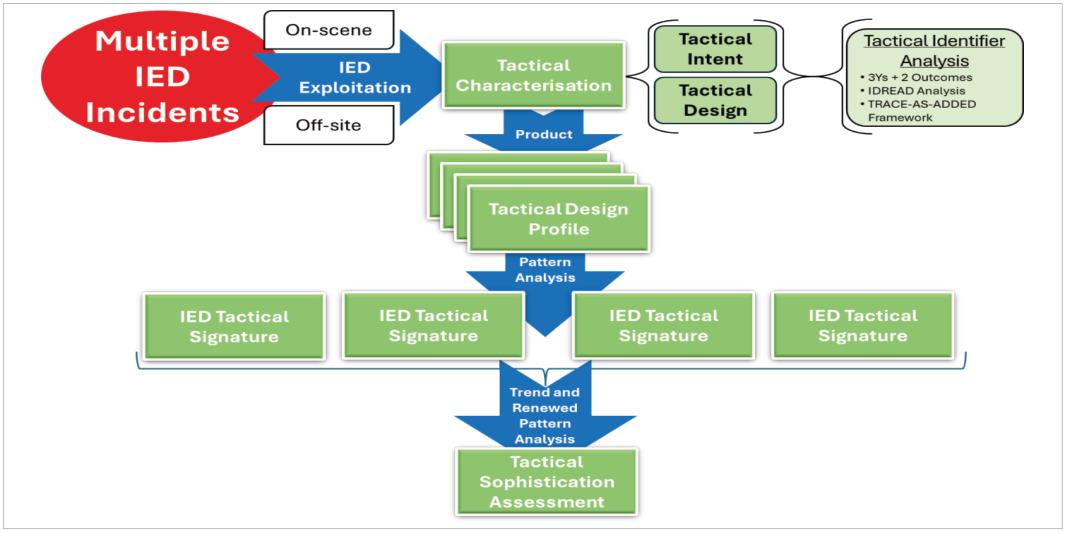
IED tactical profiles and signatures offer a powerful means to support an understanding of the tactical sophistication of an IED threat, provided they are context-specific, updated regularly to stay threat-aligned, and illustrated with real-world examples when feasible. To be effective, they also need to be handled with appropriate information security protocols and disseminated in a timely and targeted manner to those who need them

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

19 The interaction between systems that collect, process, fuse and communicate information and those that apply military force that has enabled the West to use precision violence against its foes is known as the revolution in military affairs. Source: The limits to revolutions in military affairs: Maurice of Nassau, the battle of Nieuwpoort (1600), and the legacy", by Geoffrey Parker, Journal of military history 71:2, 2007, 331-372.

20 Throughout history, each era has tended to view innovations in warfare as a form of 'revolution,' whether due to increased destructive power or a perceived affront to traditional moral and cultural values. Warfare has gradually become more 'total,' driven by forces such as state centralisation, expanded resource mobilisation, technological advancement, the application of scientific and rational methods,[A] enhanced military discipline, and the institutionalization of military education. What sets the rise of the UAS–IED nexus apart is its detachment from conventional state control. Unlike previous military revolutions that were primarily shaped by state actors and formal militaries, this shift is increasingly driven by non-state actors and even criminal networks. Despite this decentralization, its impact on the character and conduct of conflict is no less significant.

NOTE: A. Reference to 'rational methods' highlights how previous eras of warfare were shaped by institutional logic and state-sponsored innovation, whereas today's shifts are more chaotic and grassroots, yet still highly impactful.




Assessment process of the tactical sophistication of an IED threat.

most. IED incident reporting, which supports tactical device profile and tactical signature development, allows for an assessment of the tactical sophistication of an IED threat.

This, in turn, directly supports the design, development, and maintenance of an accurate IED threat picture, enabling the C-IED enterprise to better respond, counter and ideally prevent existing and emerging IED threats.

As we continue this series on the design, development and sustainment of an IED threat picture, the next article will focus on IED technical identifiers as the key data upon which IED technical profiles and subsequent IED technical signatures can be developed. The use of IED technical signatures to assess IED technical complexity will also be set out. A methodology by which IED incident profiles can be developed will also be provided. ■

## ABOUT THE AUTHOR

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

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