

INTERNATIONAL GUILD OF MASTER BOMB TECHNICIANS

Threat & Technical Analysis Cell

Global Explosive Incident Trends

A TTP and Technical Trend Analysis for CIED Practitioners

Reporting Period: 16 February – 31 May 2026

Derived from 15 consecutive Weekly Explosive Incident Briefs

UNCLASSIFIED // OPEN-SOURCE INTELLIGENCE

Audience: experienced IED / CIED, EOD, and security practitioners

Compiled 1 June 2026. All source material is publicly available.

Contents

Contents.....	2
1. Scope, Sources, and Method	3
2. Key Judgments	3
3. Quantitative Overview	5
3.1 Where: theater distribution.....	5
3.2 How: delivery and emplacement.....	5
3.3 Whom: target category.....	6
3.4 The headline trend: explosive UAS over time.....	7
4. Adversary TTP Trends	8
4.1 Explosive UAS: the defining capability shift.....	8
4.2 Vehicle-borne and proxy delivery	8
4.3 Secondary devices and responder targeting	9
4.4 Decapitation and targeted killing.....	9
4.5 Disposable and remotely recruited operators.....	9
4.6 Critical-infrastructure and economic warfare	9
4.7 Criminal-explosive normalization	10
5. Device Technical Makeup	11
5.1 Main charges and fills	11
5.2 Initiation and firing systems.....	11
5.3 Concealment and form-factor	12
5.4 Fuzing, anti-handling, and the render-safe environment.....	12
6. Regional and Threat-Actor Trajectories	14
7. Force-Protection Implications and Watch Items	16
7.1 Countermeasure gaps surfaced this period.....	16
7.2 Watch items into the next quarter	16
8. Appendix	18
8.1 Source briefs (15).....	18
8.2 Carded-set tallies	18

1. Scope, Sources, and Method

This report synthesizes 15 consecutive IGMBT Weekly Explosive Incident Briefs covering 16 February through 31 May 2026. It is written for a reader who already understands device theory, initiation systems, and counter-IED operations. The intent is not to re-list incidents but to extract the trends that matter for force protection: how adversaries are delivering and initiating devices, what those devices are made of, how each theater is evolving, and where the practitioner community should be looking next.

Source base. Each weekly brief is an open-source product built from public reporting, with per-incident confidence grading (Confirmed, Probable, Possible) and explicit reliability caveats. The briefs use an incident-card and ledger format, supplemented in most weeks by a thematic TTP-analysis section and conventional-conflict appendices. This analysis preserves that confidence discipline and does not upgrade any claim beyond what the briefs assert.

Counting method. For quantitative figures we built a consolidated record of distinct, in-window carded incidents (n = 176). Incidents that recur across consecutive briefs as reporting matures (for example the Lviv-Mykolaiv-Dnipro-Moscow police series, the Diffa-Doutchi bridge, the Gracie Mansion TATP devices, and the Netherlands antisemitic wave) are counted once, at first appearance, to avoid double-counting. Multi-site campaigns reported as a single card (for example a nationwide ELN cylinder-bomb strike, or a 30-plus-device defensive belt in southern Cauca) are counted as one record even though they represent many devices.

Known gaps. The briefs repeatedly flag under-reporting that biases any global count. Sahel-core and Mali junta media suppression, thin Somalia and Mindanao reporting, English-language search saturation that obscures Pakistani tribal-belt activity, and Sweden's criminal bombing wave (roughly 621 explosion offenses logged in 2025, the highest on record, yet rarely indexed as discrete incidents) all mean the true volume is higher than the carded count. Conventional-conflict munitions (airstrikes, artillery, missiles) are excluded by each brief's scope, though Ukraine, Gaza, Lebanon, and the 2026 Iran war recur as technology-source context. Treat the numbers here as a structured read of the carded set, not a census.

Bottom line up front. The dominant story of the period is diffusion, not novelty. The highest-impact battlefield technique of the decade, the small precision explosive drone, moved decisively into multiple non-state theaters during these 15 weeks. Around that headline, three convergences recur: responder and second-device targeting, vehicle and proxy delivery against hardened or symbolic targets, and the normalization of explosives as a tool of criminal coercion. Underneath all of it sits a structural shift the briefs name explicitly: non-state actors are buying capability with knowledge rather than materiel, defeating access controls through accessible explosives and commercial components.

2. Key Judgments

The following judgments are drawn across the full reporting period. Confidence reflects the weight and consistency of the underlying carded reporting.

- KJ-1. Explosive-drone delivery crossed from a battlefield specialty into a standing non-state capability during the period. Colombia reached an Army-stated rate above 20 explosive-drone attacks per month, Hezbollah employed a jam-immune fiber-optic FPV in Lebanon, and TTP-aligned cells dropped quadcopter munitions in Bannu. The recurring thesis, that any innovation on a high-

visibility battlefield should be expected in at least one non-state theater within about 12 months, held repeatedly. C-UAS at fixed military and critical civilian sites is now a baseline force-protection requirement, not a niche one.

- KJ-2. Responder and second-device targeting intensified and spread across unrelated actors. The Lviv double-tap (false-call lure plus secondary), Hezbollah's secondary strike on a medevac party, JNIM's pressure-plate secondary placed in the responder footprint of a civilian-target attack, and the Damascus VBIED-then-render-safe sequence all point one way: the area around a functioned device must be treated as a multi-device problem by default.
- KJ-3. Vehicle-borne and proxy delivery diversified in both form and intent, from 1,200 to 1,500 kg suicide VBIEDs in Pakistan and a decapitation VBIED against a sitting defence minister in Mali, to coerced proxy-driver devices against PSNI stations and under-vehicle magnetic IEDs used for assassination across criminal and state actors.
- KJ-4. Device construction trended toward accessible, low-signature designs: gas-cylinder main charges (Colombia, Northern Ireland, Ecuador), TATP synthesized by self-radicalized actors in the United States, and low-metallic HME and ANFO charges built to defeat metal-detector sweeps in Pakistan, the Sahel, and Myanmar. The barrier being lowered is knowledge, not access to military explosives.
- KJ-5. Initiation systems bifurcated. At the low end, SIM-rigged phone-call detonators and hobby-fuse firing trains cost a few hundred dollars per attempt. At the high end, fiber-optic command links and dual-relay WiFi/4G firing sets are explicitly engineered to defeat RF detection and electronic-warfare jamming, degrading the EW-centric C-UAS and counter-RCIED toolkit.
- KJ-6. Critical infrastructure entered the routine target set: power transmission (Mali OMVS), a municipal drinking-water dam (Alabama), dedicated freight rail (India), and ATM and cash-handling networks (Netherlands, South Africa). Several represent first-of-kind disclosures in their category.
- KJ-7. Criminal explosive use is scaling faster than insurgent use where it proves profitable. Extortion-by-explosive surfaced on three continents in a single late-May week (South Africa, Ecuador, Israel), pushing EOD demand onto civilian police forces that are often under-resourced for it.
- KJ-8. Geographic concentration held even as tactics spread. The Sahel and West Africa, the Andean ridge (Colombia especially), Pakistan's northwest and Balochistan, and Myanmar remained the persistent hotspots, while Western Europe saw a distinct, lower-lethality but politically directed campaign of placed charges against Jewish and diplomatic targets.

3. Quantitative Overview

The four figures below summarize the consolidated carded set (n = 176 distinct in-window incidents). They are a structured read of the reporting, not a global census; the gaps noted in Section 1 mean real volume, especially criminal and Sahel-core activity, runs higher.

3.1 Where: theater distribution

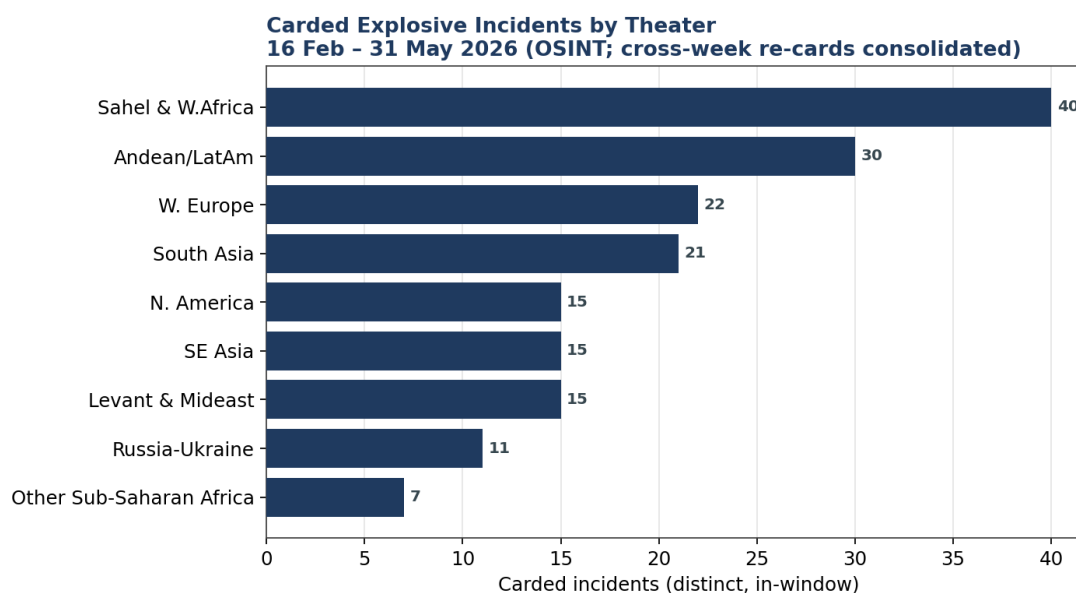


Figure 1. Distinct carded incidents by theater, 16 Feb – 31 May 2026.

The Sahel and West Africa lead the carded set (about 40 incidents), reflecting the Lake Chad Basin insurgency, JNIM's expansion in Burkina Faso and Mali, and the increasingly national spread of IED activity inside Nigeria (northeast ISWAP and Boko Haram, northwest bandit groups, and a southeastern IPOB/ESN signature). The Andean theater (about 30, almost entirely Colombia) is driven by the ELN and FARC-dissident pre-election campaign. Western Europe's share is unusually high for a low-conflict region, but its incidents are mostly low-lethality placed charges tied to the Iran-aligned antisemitic wave and to criminal bombing, a different threat shape than the Sahel or South Asia.

3.2 How: delivery and emplacement

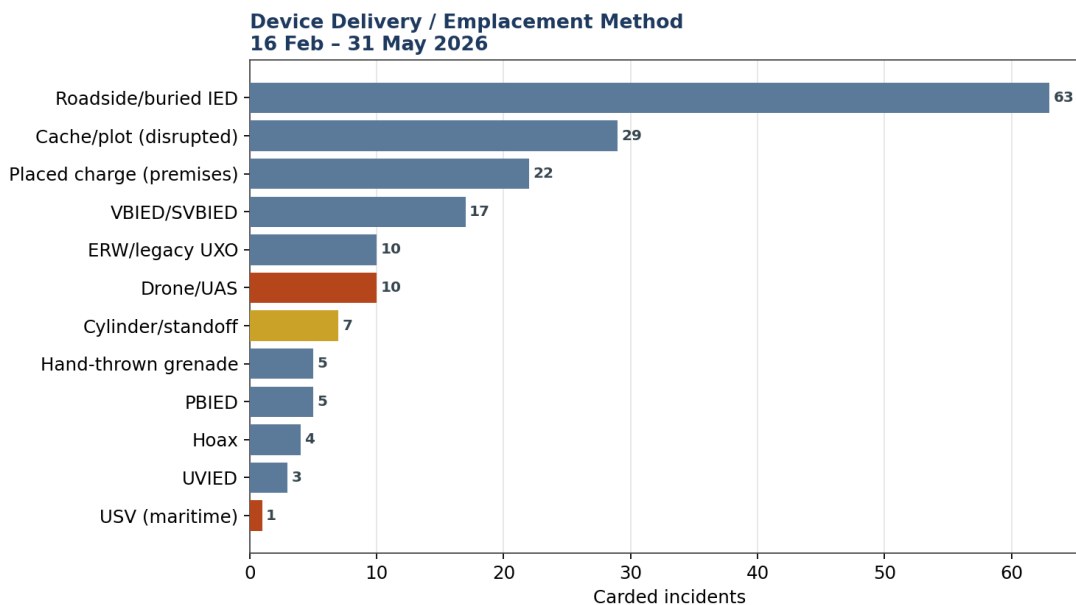


Figure 2. Device delivery / emplacement method across the carded set.

Roadside and buried IEDs (command-wire, command-pull, victim-operated, and remote roadside devices) remain the workhorse of the global IED problem and dominate the count. The large disrupted-cache and plot category reflects both genuine interdiction success and the routine domestic call-outs (United States pipe-bomb finds, legacy Maoist and Nepali stockpiles) captured by the briefs. The figures that matter for the trend story are smaller in absolute terms but rising and qualitatively significant: explosive drones and a maritime USV, gas-cylinder and standoff tatuco devices, and under-vehicle IEDs used for targeted killing.

3.3 Whom: target category

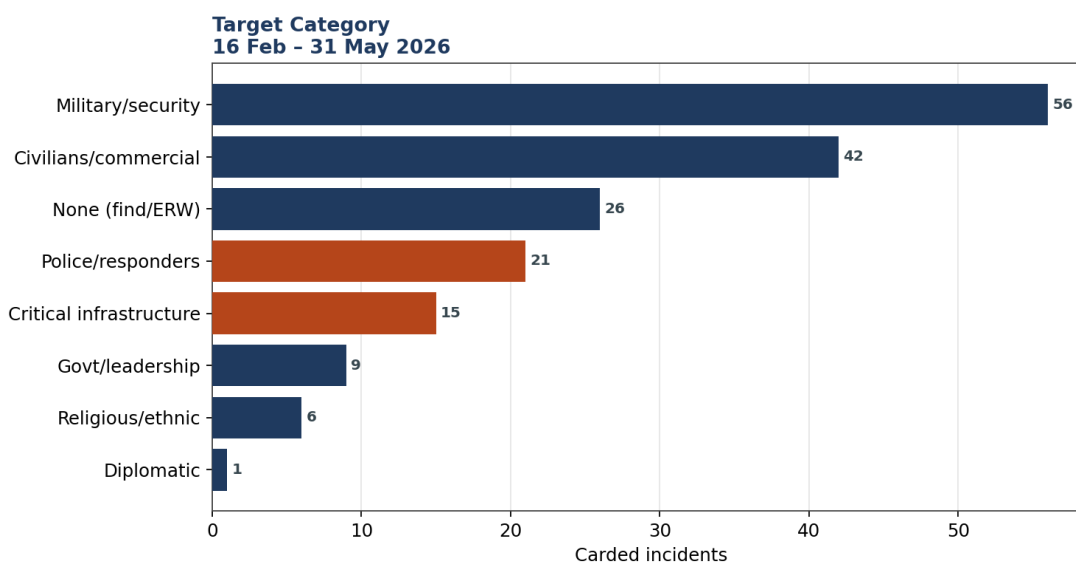


Figure 3. Target category across the carded set.

Military and security forces remain the most-targeted category, but civilians and commercial premises run a close second, and police or first responders are a distinct and deliberately chosen third. The combined civilian, commercial, police, religious, and critical-infrastructure share shows how much of the current threat falls outside the classic military-convoy model and onto soft and symbolic targets that civilian agencies must protect.

3.4 The headline trend: explosive UAS over time

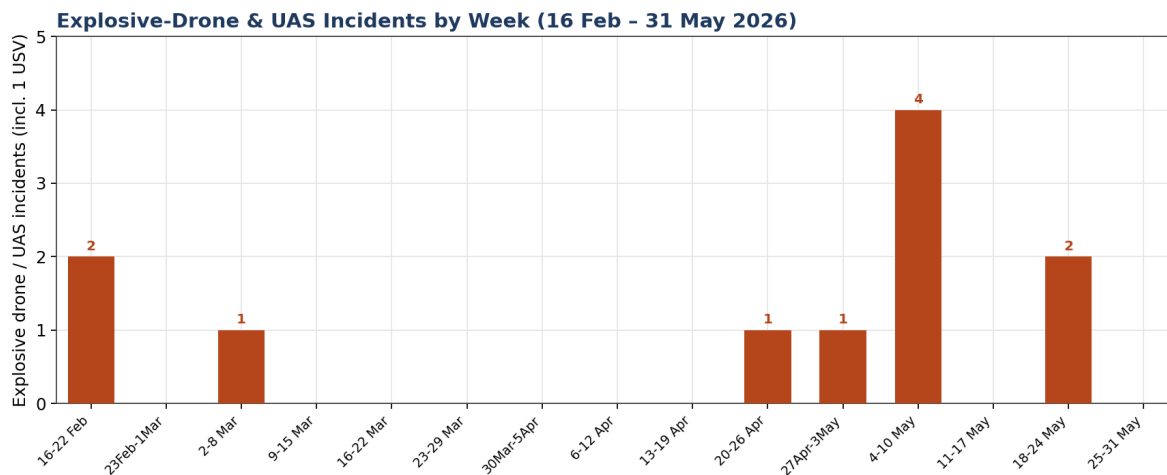


Figure 4. Explosive-drone and UAS incidents by week (includes one maritime USV).

Explosive-UAS incidents are not the largest category, but their distribution tells the clearest trend story of the period. A February baseline (the ELN's first acknowledged FPV strike in Colombia and a suicide drone against a Myanmar airport) gives way to a pronounced cluster in early-to-mid May, when fiber-optic FPVs, a C-4 quadcopter near Bogota's airport, drone drops in Pakistan, and a drifting Magura-class naval drone all appear within days. The dip in late May reflects a real lull in carded drone events, not a reversal; the underlying Colombian campaign continued at industrial scale. This is a delivery-vector innovation more than a charge innovation, and it is diffusing on a roughly 12-month cycle from source battlefields.

4. Adversary TTP Trends

4.1 Explosive UAS: the defining capability shift

Across the period the single most consequential development is the operationalization of small precision explosive drones by non-state and quasi-state actors in at least four theaters. The forms vary, but the trajectory is one of maturation from improvisation to standing capability.

Fiber-optic FPV (Lebanon). Hezbollah's 26 April Taybeh strike used a fiber-optic-guided FPV against an IDF tank crew and then launched additional explosive-laden drones at the medevac party. The fiber tether (effective to roughly 10 to 30 km, described as dental-floss-thin) is immune to RF jamming and carries negligible thermal or radar signature. The trainer and technology pipeline traces to Ukrainian fiber-optic FPV practice, a transfer of under 24 months. The operational lesson is blunt: RF-detection and EW-jamming C-UAS will not defeat a tethered FPV; physical defeat (nets, wires, kinetic) and acoustic or optical sensing become primary.

Industrialized drone-IED (Colombia). Colombia moved from a single acknowledged FPV attack in February to an Army-stated rate above 20 explosive-drone attacks per month by late May. Devices ranged from gravity-released grenade drops to a fiber-optic-guided FPV carrying 260 g of C-4 in a PVC tube with a syringe-rigged detonator and onboard camera, recovered under 6 km from Bogota's international airport. Simultaneous multi-site drone attacks in southern Bolivar indicate command-level synchronization and a shared logistics and training pipeline across dissident structures.

Quadcopter drop (Pakistan) and maritime USV (Mediterranean). A TTP-aligned cell dropped a quadcopter munition on a Bannu residential area, a method that defeats blast walls and costs far less than a VBIED. Separately, a Magura V3-class naval drone (manufactured platform, multiple detonators, reported charge from tens to hundreds of kilograms) drifted out of the Black Sea operational area and was recovered by fishermen off Lefkada, the first publicly documented USV recovery outside the Black Sea or Azov, and a warning that nation-state-grade maritime IEDs can wash up where untrained civilians handle them.

4.2 Vehicle-borne and proxy delivery

Mass and decapitation VBIEDs. Suicide VBIEDs scaled in both yield and ambition: a 1,200 to 1,500 kg main charge at Bannu, a vehicle bomb timed to a passing passenger train at Quetta (23-plus killed, BLA's third major rail or transport strike of 2026), and a VBIED that killed the Malian defence minister's family members at his residence, the highest-profile improvised decapitation attempt against a sitting government in the period. These require detailed pre-attack ISR on the target's pattern of life.

Proxy-driver and hijacked-vehicle devices. Dissident republicans in Northern Ireland ran at least two coerced proxy-driver attacks (Lurgan and Dunmurry) using gas-cylinder charges in hijacked vehicles against PSNI stations, reactivating a 1970s-90s Provisional-era technique. The proxy model shifts delivery risk onto a civilian and creates a hard ROE problem (a hostile vehicle with a possibly hostage driver) that complicates neutralization.

Under-vehicle IEDs for assassination. Magnetic-clamp and under-chassis devices recurred across very different actors: Ukrainian GUR operations in occupied Crimea and Sevastopol, an FSB-attributed under-vehicle device in Dnipro initiated by a phone call to a SIM-rigged detonator, and cartel attacks on prosecutors in Mexico and now Bolivia. Tradecraft is converging on small, magnetic, motion- or remote-actuated devices.

New vehicle form-factors. Pakistan saw a rickshaw-borne IED in a crowded Lakki Marwat bazaar and persistent motorcycle-borne devices; motorcycle delivery recurred as a convergent platform choice across Pakistan, Nigeria, Mali, Colombia, Syria, and Thailand, selected independently for the same reasons (cheap, disposable, low-observable).

4.3 Secondary devices and responder targeting

The clearest cross-theater TTP convergence after drones is deliberate targeting of responders. The Lviv attack used a false store-break-in call to lure a patrol onto a primary device, with a second device for backup and EMS. Hezbollah struck a medevac party after an initial FPV hit. In Mali, JNIM emplaced a pressure-plate secondary in the expected responder footprint of a primarily civilian-target attack, the first such instance in the period where the secondary was sited for civilian first responders rather than military EOD. The Damascus Bab Sharqi sequence (VBIED then a separately planted IED) produced the classic render-safe trap. The practitioner implication recurs in the briefs: a second cordon sweep and a deliberate search for secondaries must precede manual approach, and the detonation site should be treated as a multi-device zone with an expanded search radius.

4.4 Decapitation and targeted killing

Beyond the Mali minister VBIED, the period shows a sustained pattern of targeting named individuals and local leadership: a tribal-chief assassination by a vehicle-keyed IED in a Wana market, ISWAP killing a CJTF commander with a route-predicted command IED near Baga, and intra-ISWAP fratricide by emplaced IED. Targeting people who can identify fighters or broker local governance (jirga leaders, militia commanders) is an intelligence-denial strategy, and it makes the movement patterns of auxiliaries and local notables a priority emplacement-prediction problem.

4.5 Disposable and remotely recruited operators

A recruitment-and-tasking model matured throughout the period: adversaries recruit financially desperate, often young or apolitical individuals through Telegram, Snapchat, and other messaging apps, direct them by encrypted comms to a pre-positioned cache, and initiate remotely, sometimes without the carrier's full knowledge. It appears in the Russia-Ukraine shadow war (Telegram-recruited operatives, SIM-rigged triggers, and a camera set up to livestream the strike as a propaganda asset, at a few hundred dollars per attempt), in the use of minors paid 500 to 1,000 euros in Paris, and in self-radicalized young actors synthesizing TATP in the United States. The defensive consequence is that pre-attack indicators increasingly live in social-media and financial behavior rather than in physical surveillance of a trained cell.

4.6 Critical-infrastructure and economic warfare

Infrastructure targeting recurred almost weekly by late spring. JNIM shifted toward economic strangulation of Bamako, attacking the Manantali OMVS power-transmission line and threatening the hydroelectric plant. An IED was placed against the Converse Reservoir dam in Alabama, described as the first publicly disclosed IED placement against a US municipal drinking-water dam in recent memory. India saw repeated sabotage of the Dedicated Freight Corridor. The Netherlands and South Africa saw explosive attacks on ATM, cash-deposit, and retail networks. These targets share a force-protection blind spot: subsurface, submerged, and after-hours access points that conventional perimeter security does not cover.

4.7 Criminal-explosive normalization

The briefs make a structural argument worth taking seriously: criminal explosive use scales faster than insurgent use once it proves profitable, and it pushes EOD demand onto civilian police forces. The late-May window showed extortion-by-explosive converging on three continents at once (overnight no-casualty IEDs at South African Woolworths stores, grenade and IED attacks on Ecuadorian businesses, and assassination-style car bombs in Israel), against a backdrop of Sweden's record bombing rate and endemic Andean extortion bombing in Peru and Ecuador. The diagnostic signature is an overnight, low-casualty device at a commercial premises, followed by a demand.

5. Device Technical Makeup

This section consolidates the device-level detail most relevant to render-safe planning, exploitation, and detection. The through-line is a deliberate bias toward components that are cheap, available, and hard to detect, combined with selective high-end engineering where the adversary is contesting the electromagnetic spectrum.

5.1 Main charges and fills

Charge / fill	Where it appeared and why it matters	Detection note
Gas-cylinder / cylinder bomb	Colombia (tatuco / rampa, launched or emplaced), Northern Ireland (hijacked-vehicle main charge), Ecuador (gas-cylinder builds, some lacking functional HE). Cheap, durable, hard to spot casually, forgiving of imperfect fills; doubles as standoff projectile and emplaced road charge.	Steel body gives a strong metallic signature but the form blends into normal cargo; the launch point, not the impact point, may hold the firing link.
Low-metallic HME / ANFO	BLA in Balochistan, JNIM in the Sahel, PDF in Myanmar (PVC-bodied ANFO and sugar-fuel mixes). Polyether-bonded or emulsion fills with minimal metal content.	Designed to defeat metal-detector and magnetic sweeps; drives a shift to GPR and route pattern-of-life on high-value routes.
TATP (peroxide)	Self-radicalized actors, United States (Gracie Mansion mason-jar devices, plus a Bucks County cache). Hobby-fuse and M80 initiation; externally taped nuts and bolts for fragmentation.	Primary-explosive sensitivity and instability; partial functions are quality-control failures, not lack of intent. Default to TATP contamination protocols on ISIS-inspired US responses.
Military / commercial HE	Hezbollah (directional and EFP-class legacy devices), Colombian C-4 drone payload (260 g), diverted mining emulsions and PETN det cord (JNIM infrastructure attacks).	Higher order and directional effects; EFP and shaped-charge re-emergence is the key escalation indicator in the Levant.
Repurposed ordnance / projectiles	Mortar rounds (60/82 mm) as IED main charges (Myanmar), recovered artillery projectiles (Nigeria), anti-tank / shaped-charge recoveries (IPOB Enugu).	Sympathetic-detonation hazard during render-safe; indicates supply from battlefield recovery or diversion.

5.2 Initiation and firing systems

Initiation is where the period's bifurcation is sharpest. The low end is cheaper and more scalable than ever; the high end is explicitly engineered to defeat the counter-RCIED and C-UAS toolkit.

Initiation	Representative use	Implication for the operator
Command-wire / command-pull	BLA and JNIM on narrow predictable routes; persistent across the Sahel and Pakistan.	Short standoff, no RF emission; ECM is irrelevant. Address by route domination and visual search.
Phone / SIM-rigged RC	Lviv waste-bin IEDs, Dnipro under-vehicle device (call to a SIM-rigged detonator), Tehran LPG-cylinder RCIEDs.	Low-cost, reproducible, a few hundred dollars per attempt; vulnerable to RF jamming, which is why higher-end actors are moving off it.
Fiber-optic guidance	Hezbollah FPV (Lebanon), Colombian C-4 FPV. Tether to 10–30 km.	Immune to RF jamming and EW; defeats RF-based C-UAS. Requires physical or acoustic/optical defeat.
Dual-relay WiFi/4G	Moscow e-scooter WBIED (1.5 kg PE, bolt-and-nut frag, smart-home WiFi plus 4G modem).	Built-in redundancy against single-band jamming; a documented step up in counter-jam sophistication.
Victim-operated / pressure	Myanmar, Nigeria, Maoist India, Sahel; pressure-plate secondaries in responder footprints.	Indiscriminate and persistent; the legacy-ERW tail keeps killing clearance teams and civilians for years.
Suicide / self-initiated	PBIED and SVBIED in Pakistan and Nigeria (Maiduguri triple PBIED, Quetta train, Bannu).	Defeats command-link countermeasures entirely; behavioral and access-control indicators are the main defense.

5.3 Concealment and form-factor

Concealment trended toward objects that read as ordinary in their environment: waste bins on a city street, a fire extinguisher outside a supermarket, a backpack on a public trail, a rickshaw in a bazaar, a commercial electric scooter outside a business center, ATM and storefront housings after hours, and gas cylinders that pass as cargo. The common defensive failure mode is that each blends into a specific everyday setting, defeating generic suspicious-object cueing. The recurring instruction in the briefs is to teach environment-specific baselines (what normal looks like at a checkpoint, a bazaar, a station forecourt) rather than relying on a universal device silhouette.

5.4 Fuzing, anti-handling, and the render-safe environment

Several threads bear directly on render-safe planning. Colombian EMC devices increasingly pair a primary timer with a secondary anti-tampering element, and cylinder devices pack layered fragmentation in the annular space around a central booster. Standoff tatuco barrages produce high dud rates (about 75 percent at

Riohacha, where 9 of 12 projectiles required render-safe), so a single standoff attack generates a UXO-clearance problem an order of magnitude larger than the detonation itself. Legacy buried devices repeatedly killed clearance teams on accidental circuit closure during recovery (Chhattisgarh, Zanzan), arguing for a bias toward in-place disruption over recovery. And submerged or subsurface placement (the Alabama dam) puts devices outside the reach of standard EOD approach techniques.

6. Regional and Threat-Actor Trajectories

Theater	Trajectory over the period	Signature devices / actors
Sahel & West Africa	Highest carded volume. JNIM shifted from static-post attacks toward route interdiction and economic warfare (power, fuel, movement) and a decapitation VBIED in Bamako. Nigeria's IED problem went national: NE ISWAP/Boko Haram, NW bandits adopting jihadist TTPs, and a SE IPOB/ESN signature including anti-tank recoveries. Boko Haram demonstrated a renewed mass-casualty PBIED capability in Maiduguri.	Roadside/buried IEDs, command and VO; mortar and projectile main charges; armed drones (ISWAP); PBIED revival.
Andean (Colombia)	Pre-election ELN and FARC-dissident campaign escalated from standoff harassment to mass-casualty civilian-transport attacks and an industrialized explosive-drone capability (>20/month). Criminal extortion bombing persists in Ecuador and Peru.	Cylinder/tatuco bombs, motorcycle delivery, FPV and gravity-drop drones, anti-tamper EMC devices.
South Asia (Pakistan)	Sustained TTP and BLA campaign in KP and Balochistan: large suicide VBIEDs, rickshaw and motorcycle IEDs, SHO/leadership targeting, a rail-corridor campaign, and emerging quadcopter drops. Low-metallic charges defeat detector sweeps.	SVBIED (1.2–1.5 t), RCIED/VOIED, low-metallic HME; BLA command-pull roadside devices.
Levant & Mideast	Hezbollah fielded jam-immune fiber-optic FPVs and buried directional devices against the IDF; ISIS remnants used VBIED-plus-secondary in Damascus. The 2026 Iran war drove proxy activation and ERW/UXO clearance casualties (Zanjan).	Fiber-optic FPV, EFP/directional legacy, LPG-cylinder RCIED (Iran), VBIED + secondary.
Russia–Ukraine	Shadow war centered on recruited disposable operators: Telegram tasking, SIM-rigged and under-vehicle devices, e-scooter WBIED with dual-relay anti-jam initiation. Officer assassinations continue.	UVIED, RCIED, dual-relay WiFi/4G; recruited-minor and contracted-national model.
W. Europe	Two distinct strands: an Iran-aligned, low-lethality placed-charge campaign against Jewish and diplomatic targets (Ashab al-Yamin), and criminal bombing (Sweden, Netherlands ATMs). Dissident-republican proxy VBIEDs in N. Ireland. Rising WWII ERW encounter rate.	Placed charges/incendiary at premises, gas-cylinder proxy VBIED, ATM gas/solid charges, legacy ERW.
SE Asia	Persistent low-intensity VOIED campaigns: Myanmar PDF pressure-plate devices (civilian bycatch) and Thailand's BRN deep-south harassment. A grievance pipe-bomb in Baguio was the period's worst non-conflict single IED.	Pressure-plate VOIED, padesa command mines, commercial/pipe IEDs.
N. America	Mostly domestic finds, caches, and hoaxes, plus a confirmed TATP threshold event (Gracie Mansion) and a critical-infrastructure first (Alabama dam).	Pipe bombs, TATP, hoax mock-IEDs.
Other Sub-Saharan Africa	Escalation indicators to watch: ADF (DRC) and ISM (Mozambique, Macomia roadside IED vs convoy) following the opportunistic-to-systematic curve seen	Roadside IEDs, extortion IEDs, combined assault-plus-IED.

Theater	Trajectory over the period	Signature devices / actors
	earlier in the Sahel and Somalia; South African extortion bombing.	

7. Force-Protection Implications and Watch Items

The following are the practitioner-facing consequences that recur across the briefs, framed as what to change and what to watch.

7.1 Countermeasure gaps surfaced this period

- **C-UAS is now baseline, and RF-only C-UAS is insufficient.** Fiber-optic and dual-relay firing trains defeat RF detection and jamming. Fixed military and high-value civilian sites need layered C-UAS that includes acoustic, optical, and physical (net, wire, kinetic) defeat, plus a plan to exploit recovered drone payloads and fuze trains.
- **Treat every functioned device as a multi-device scene.** Lure-and-double-tap, medevac strikes, and pressure-plate secondaries in responder footprints all argue for a deliberate secondary search and an expanded standoff before manual approach, including for civilian-target attacks where responder targeting is now demonstrated.
- **Detection must assume low-metallic and cylinder charges.** Metal-detector-defeating HME and ANFO on predictable routes call for GPR, route domination, and pattern-of-life analysis rather than sweep-and-go. The launch point of a standoff cylinder attack may hold the firing link.
- **Critical-infrastructure access points are under-protected.** Subsurface, submerged, and after-hours access (dams, transmission towers, rail, ATM and retail housings) sits outside conventional perimeter security. Utilities should re-look subsurface and submerged inspection regimes and pre-coordinate with EOD.
- **Pre-attack indicators have moved online.** Recruited-operator and minor-courier models mean financial and social-media behavior, not physical cell surveillance, is often the earliest warning. Monitoring of recruitment platforms and proxy-driver/hijack reporting is a force-protection input.
- **Standoff barrages create outsized UXO problems.** High dud rates turn one tatuco attack into a multi-item render-safe task. Plan clearance resourcing for the duds, not just the detonation.

7.2 Watch items into the next quarter

- Further proliferation of fiber-optic and tethered FPVs to Iran-aligned proxies and additional non-state actors on a sub-12-month cycle.
- Continuation of the Pakistan KP and Balochistan VBIED and rail campaign, and standardization of BLA vehicle profiles and charge sizes.
- Post-election Colombian tempo: whether the ELN and FARC-dissident drone campaign sustains or escalates after the May electoral cycle.
- ISM (Mozambique, Cabo Delgado) and ADF (DRC) moving from opportunistic to systematic roadside-IED use, the clearest regional escalation indicators.
- Spread of the recruited-disposable-operator and proxy-driver models from the Russia-Ukraine and Northern Ireland contexts to wider European soft targets.
- Normalization of extortion-by-explosive in South Africa, Ecuador, and beyond, with EOD demand landing on civilian police.

- Persistence of ammonium-nitrate precursor plots against Israeli and Jewish targets in Mediterranean and Western Europe.

8. Appendix

8.1 Source briefs (15)

This analysis is derived from the following IGMBT Weekly Explosive Incident Briefs. All are open-source products; individual incidents carry the confidence grades assigned in each brief.

1. Explosive Incident Brief for the Week of 16 – 22 February 2026
2. Explosive Incident Brief for the Week of 23 February – 1 March 2026
3. Explosive Incident Brief for the Week of 2 – 8 March 2026
4. Explosive Incident Brief for the Week of 9 – 15 March 2026
5. Explosive Incident Brief for the Week of 16 – 22 March 2026
6. Explosive Incident Brief for the Week of 23 – 29 March 2026
7. Explosive Incident Brief for the Week of 30 March – 5 April 2026
8. Explosive Incident Brief for the Week of 6 – 12 April 2026
9. Explosive Incident Brief for the Week of 13 – 19 April 2026
10. Explosive Incident Brief for the Week of 20 – 26 April 2026
11. Explosive Incident Brief for the Week of 27 April – 3 May 2026
12. Explosive Incident Brief for the Week of 4 – 10 May 2026
13. Explosive Incident Brief for the Week of 11 – 17 May 2026
14. Explosive Incident Brief for the Week of 18 – 24 May 2026
15. Explosive Incident Brief for the Week of 25 – 31 May 2026

8.2 Carded-set tallies

Counts of distinct in-window carded incidents (n = 176), with cross-week re-cards consolidated. Provided for transparency; see Section 1 for the gaps that bias any global reading.

Delivery method	Count	Target category	Count
Roadside / buried IED	63	Military / security	56
Disrupted cache / plot	29	Civilians / commercial	42
Placed charge (premises)	22	None (find / ERW)	26
VBIED / SVBIED	17	Police / first responders	21
Explosive drone / UAS	10	Critical infrastructure	15
ERW / legacy UXO	10	Government / leadership	9
Cylinder / standoff (tatuco)	7	Religious / ethnic	6
PBIED	5	Diplomatic	1
Hand-thrown grenade	5		
Hoax	4		
Under-vehicle IED	3		
Maritime USV	1		

Prepared by the IGMBT Threat & Technical Analysis Cell. UNCLASSIFIED // OSINT. Distribution per originator.