



SECURITY UPDATE / NORTH AFRICA & CRITICAL INFRASTRUCTURE

Libya: Zawiya UAV Attacks and Benghazi Intelligence Assassination

Oil and gas infrastructure exposure, militia instability and commercial counter-UAV planning

Assessing the Zawiya refinery and power plant UAV strikes, the targeted killing of a senior Libyan intelligence officer, and practical implications for oil, gas, remote operations and critical infrastructure security.

FOCUS

Zawiya refinery | Benghazi | UAV threat | Oil & gas infrastructure

Militia instability | Critical infrastructure protection | Commercial counter-UAV planning

EXECUTIVE ASSESSMENT

Executive Summary

The 10-11 August 2026 UAV attacks against Zawiya's oil and power infrastructure and the separate car-bomb assassination of Maj. Gen. Fawzy al-Mansouri in Benghazi show that Libya's security environment remains fragmented, militia-driven and highly exposed to both conventional and emerging threats. The Zawiya incident is particularly significant because it demonstrates how relatively low-cost unmanned aerial systems can generate strategic effect against oil and gas infrastructure without requiring a large armed force, direct occupation of a facility or sustained ground combat.

The Zawiya attack involved explosive-laden drones striking fuel storage and power infrastructure in one of Libya's most important western energy hubs. A gasoline tank holding approximately 4.5 million litres of fuel collapsed after being hit, while additional drones reportedly struck or landed near the town's power plant and fuel storage areas. Libya's National Oil Corporation declared a state of maximum emergency at the facility and warned that it could declare force majeure or halt operations if attacks against the Zawiya complex continued. The refinery has a capacity of approximately 120,000 barrels per day and is linked to the 300,000 barrel-per-day Sharara oilfield, making the incident operationally significant beyond the immediate fire damage.

The Benghazi attack was different in character but equally significant. Maj. Gen. Fawzy al-Mansouri, the head of military intelligence for Khalifa Haftar's eastern-based Libyan National Army, was killed when an explosive device detonated in or near his vehicle on 10 August. No group has claimed responsibility. Reporting places the attack in Benghazi, although the exact neighbourhood has been described differently by major sources. This discrepancy does not change the core assessment: a senior intelligence figure in eastern Libya was successfully targeted inside the Libyan National Army's main security area.

Together, the two incidents should not be treated as proof of a single coordinated campaign across Libya. There is no verified evidence linking the Zawiya drone attacks to the Benghazi assassination. However, they occurred in the same reporting cycle and point to the same underlying problem: Libya's divided governance, militia networks and contested control of strategic infrastructure continue to create opportunities for sabotage, targeted killing and economic disruption.

INCIDENT SNAPSHOT

Key Incident Snapshot

INCIDENT	LOCATION	OPERATIONAL SIGNIFICANCE
UAV strikes against Zawiya refinery and power plant	Zawiya, western Libya	Demonstrates exposure of oil, power and emergency response infrastructure to low-cost aerial attack.
Car-bomb assassination of Maj. Gen. Fawzy al-Mansouri	Benghazi, eastern Libya	Shows continuing vulnerability of senior security figures inside the Libyan National Army's core operating area.
Wider risk theme	National	Fragmented governance, militia networks and contested infrastructure control continue to create sabotage and targeted-killing opportunities.

OPERATING CONTEXT

Background

Libya remains divided between rival political and military power centres. The internationally recognised Government of National Unity in Tripoli continues to operate in western Libya under Prime Minister Abdul Hamid Dbeibah, while eastern Libya is dominated by Khalifa Haftar and the Libyan National Army, aligned with the Benghazi-based authorities. Libya's political crisis remains unresolved following the failure to hold national elections in December 2021, and competition between armed groups for control of territory, revenue and infrastructure continues to threaten national stability.

Zawiya is a particularly sensitive location because it combines urban militia politics with nationally important oil infrastructure. The city sits west of Tripoli on the Mediterranean coast and hosts Libya's largest operating refinery, an export terminal, fuel storage and power infrastructure. Control of Zawiya has long been contested by armed groups that are sometimes formally linked to state institutions but retain independent command structures and local economic interests.

The city has repeatedly experienced clashes affecting the refinery and surrounding infrastructure. In May 2026, fighting near Zawiya forced refinery disruption and raised warnings from the United Nations Support Mission in Libya that armed activity around strategic infrastructure could produce severe humanitarian and economic consequences. The latest UAV attacks therefore fit an existing pattern: Zawiya's oil infrastructure is not only an economic asset, but also a pressure point in western Libya's militia competition.

RECENT DEVELOPMENTS

Zawiya UAV Strikes

The first major strike occurred on 10 August 2026, when a UAV hit a gasoline tank at the Zawiya oil refinery. The tank reportedly contained approximately 4.5 million litres of fuel and collapsed after the strike. The resulting fire burned through the night and remained active into Tuesday afternoon. No casualties were reported, but the scale of the fire forced the National Oil Corporation to declare a state of maximum emergency at the facility.

Further UAV activity continued on 11 August. One drone reportedly struck near another key oil tank without causing casualties or major damage. Two additional drones hit the Zawiya power plant. One damaged firefighting infrastructure, while another landed near a fuel tank. This is especially important because it suggests the threat was not limited to direct ignition of fuel storage. The attack also affected emergency response capability. For oil and gas sites, a strike against firefighting infrastructure can be as serious as a strike against product storage because it reduces the facility's ability to contain secondary fires, cascading failures and environmental release.

Emergency and safety teams later brought the fires under control earlier than expected. Engineers indicated that the blazes had not damaged the refinery itself, but the incident caused partial shutdown of operations at the Zawiya oil depot and disrupted fuel supply to several stations in western Libya before supply resumed. The National Oil Corporation warned that it could completely halt operations at Zawiya if drone attacks against energy assets continued.

The attack has wider economic relevance. Libya has Africa's largest proven oil reserves and has recently increased output after years of disruption. That recovery remains fragile. A UAV attack that

threatens Zawiya does not need to destroy the refinery to affect investor confidence, local fuel supply, insurance, and the perception that Libya can protect critical energy infrastructure.

Local Power Dynamics Around Zawiya

The Zawiya attacks occurred amid rising tensions between the Tripoli-based government and Mohamed Bahroun, also known as Al-Far, a local powerbroker associated with armed influence in the city. Reporting has described Bahroun as controlling or heavily influencing Zawiya, although the city's actual security landscape is fragmented and contested. Analysts have assessed that Bahroun's forces may be under pressure from the western government and could resort to disruptive measures.

Attribution remains unconfirmed. No group has claimed responsibility for the drone strikes. It would therefore be inaccurate to state definitively that Bahroun, his affiliates, rival militias, the Tripoli authorities, or any eastern actor conducted the attack. The more reliable assessment is that the incident reflects a high-risk local security environment in which armed groups have both motive and access to systems capable of striking infrastructure.

The incident also highlights a specific weakness in oil and gas operations in fragmented states. Refineries, tank farms, pipelines and power plants are fixed, exposed and difficult to relocate. Armed groups understand that even limited disruption can generate political pressure, economic leverage and public fear. A single UAV strike can create a visible fire, interrupt supply, force emergency shutdowns, and undermine confidence in the state's ability to protect national assets.

TARGETED KILLING

Benghazi Car-Bomb Assassination

The Benghazi incident targeted a different centre of gravity. Maj. Gen. Fawzy al-Mansouri, the director of military intelligence for the Libyan National Army, was killed on 10 August when an explosive device detonated in or near his vehicle. Reporting places the attack in Benghazi, although the exact location has been described differently, with some sources reporting Hawari and others reporting the Sayyida Aisha neighbourhood. No group has claimed responsibility.

This was a high-value targeted killing. Al-Mansouri's position made him central to the Libyan National Army's internal security apparatus, intelligence collection, counterintelligence and monitoring of hostile networks. A successful attack against such a figure is significant because it demonstrates either insider knowledge, surveillance capability, or freedom of movement sufficient to place an explosive device near a senior target.

The attack does not necessarily indicate a collapse of Libyan National Army control in Benghazi. However, it does show that targeted assassination remains a viable threat even in areas under strong security control. The absence of a claim of responsibility makes attribution difficult. Possible explanations include internal rivalry, revenge by hostile factions, Islamist-linked remnants, criminal networks, or political actors seeking to weaken Haftar's security structure. None can be confirmed at this stage.

STRATEGIC ASSESSMENT

Security Significance

The two incidents should be assessed as evidence of a deteriorating infrastructure and leadership-security environment rather than as isolated criminal events. Zawiya shows that western Libya's energy infrastructure is vulnerable to UAV-enabled sabotage. Benghazi shows that eastern Libya's security leadership remains vulnerable to targeted attack. The incidents occurred in different regions, against different targets, and likely within different conflict networks, but together they reinforce the same conclusion: Libya remains a high-risk operating environment for energy, infrastructure, logistics and foreign commercial activity.

The Zawiya attack is the more important incident for commercial operators. It shows that UAVs can reach high-consequence targets, cause major emergency response activity, and threaten continuity of supply. It also shows that firefighting systems, power supply, fuel tanks and storage areas must be treated as interconnected security targets. A UAV attack does not need to destroy a refinery unit to create significant consequences; hitting a tank, firewater system, power plant, control cable route or pump station may be enough to force shutdown or emergency isolation.

The Benghazi assassination is more important for political and security forecasting. It suggests that the Libyan National Army's internal security environment remains contested and that senior figures may be exposed to targeted attacks. If further assassinations follow, the east could experience internal tightening, arrests, reprisals, or factional suspicion. That would increase the risk to travel, meetings, accommodation and movement around Benghazi, particularly for individuals linked to government, oil, infrastructure, military contracting or international engagement.

UAV THREAT

Relevance to Oil, Gas and Critical Infrastructure

The Zawiya attack should be treated as another example of UAV threats moving from battlefield use into critical infrastructure risk. The Ukraine conflict has accelerated this trend. In Ukraine, drones evolved rapidly from reconnaissance and artillery spotting tools into FPV strike systems, long-range one-way attack platforms, naval drones, and deep-strike systems used against refineries, depots, airfields, ships and logistics nodes. The lesson for commercial organisations is not that every company must prepare for battlefield-level drone warfare, but that the technology cycle has moved faster than traditional corporate security planning.

UAVs are attractive to hostile actors because they are relatively cheap, adaptable and difficult to detect reliably at low altitude. They can be used for surveillance, intimidation, payload delivery, explosive attack, arson, perimeter probing, or disruption of emergency response. There is no single universal counter-UAV solution. A credible response requires layered detection, assessment, reporting, consequence reduction and rehearsed emergency action.

For oil and gas, the most vulnerable locations are tank farms, loading gantries, power generation areas, substations, control rooms, pipeline valve stations, firewater pumps, communication towers, accommodation camps, remote operating sites, helipads, ports and marine terminals. These are often open, fixed and geographically exposed. In remote locations, response times are longer, police or military support may be limited, and the site may rely heavily on local guards who have never been trained to identify or respond to a UAV threat.

The key point is that most commercial organisations cannot lawfully or practically shoot down drones. Military and national enforcement agencies have access to counter-drone technologies that commercial operators usually do not, including electronic warfare, jamming, spoofing, directed disruption, kinetic interception and integrated air-defence systems. In many jurisdictions, active defeat measures are legally restricted because they can interfere with aircraft, communications, public safety or national airspace control.

This means commercial operators should focus on what is viable: early warning, reporting, site hardening, emergency response, liaison with authorities, consequence reduction and rehearsed drills. Where operations are high risk, near critical infrastructure, or located in conflict-affected areas, the best option is to request government, military, police or national security agency support in advance. A commercial site can buy cameras, radar, RF detection and procedures; it usually cannot legally run an integrated counter-drone defeat system.

PLANNING AREA	COMMERCIALLY VIABLE MEASURE	LIMITATIONS
Detection	Visual observers, CCTV, thermal cameras, acoustic sensors, RF detection, radar or multi-sensor alerting depending on site risk.	Detection does not equal defeat; it only creates time for response if procedures are rehearsed.
Consequence reduction	Protect fire pumps, generators, control rooms, communication nodes, fuel systems and emergency routes.	Hardening reduces exposure but cannot guarantee protection from all UAV types.
Agency support	Pre-arranged police, military, civil aviation or national security liaison for high-risk periods.	State agencies usually control jamming, interception and airspace enforcement powers.
Training and drills	Guards, supervisors, drivers, control-room staff and emergency teams rehearse UAV sighting and impact response.	Procedures fail if staff only receive paper instructions and do not practise under realistic conditions.

COUNTER-UAV MEASURES

Viable Measures for Commercial Organisations

Commercial counter-UAV planning should begin with a site-specific threat and vulnerability assessment. This should define likely drone types, likely launch areas, approach routes, line-of-sight positions, target attractiveness, operating hours, existing airspace restrictions, nearby communities, and realistic hostile actor capability. Oil and gas operators should not buy technology first and write procedures later. The correct sequence is threat assessment, operational requirement, legal review, agency liaison, detection concept, response plan, drills, and only then procurement.

For commercial operators, reducing exposure and limiting consequences is often more realistic than attempting to actively defeat a drone in flight. Sites should review overhead exposure of control rooms, generators, fire pumps, main electrical switch rooms, communications equipment, accommodation, fuel tanks and loading areas. In some cases, screens, netting, blast film, protective roofing, stand-off distances, earth berms, strengthened pump shelters, protected firewater loops and redundant power supply may reduce consequences. These measures will not stop every UAV, but they can prevent a small drone from creating a site-wide emergency.

The most viable technical measure for commercial sites is detection and alerting. Depending on the site, this may include trained visual observers, CCTV with elevated views, thermal cameras, acoustic sensors, RF detection, radar, or multi-sensor detection systems. Detection alone is useful if it creates time to stop hot work, move personnel under cover, isolate fuel transfer, shut exposed operations, alert firefighting teams, and notify authorities.

Operational controls are equally important. Sites should define what happens when a drone is sighted. This should include who confirms the sighting, who raises the alarm, who informs the control room, who contacts police or military liaison, who stops non-essential movement, who moves personnel to shelter, who isolates fuel transfer, and who records evidence. The biggest weakness in many commercial settings is not lack of equipment, but lack of a rehearsed decision process.

Training and drills are essential. Guards, drivers, control-room operators, supervisors and emergency response teams should know the difference between a nuisance drone, surveillance drone and possible weaponised drone. They should know what to report: direction, height estimate, sound, lights, number of drones, behaviour, payload appearance, launch direction if visible, whether it is loitering or diving, and whether there are secondary drones. They should also know what not to do: do not fire at the drone, do not crowd around the suspected impact area, do not pick up debris, and do not assume a single drone means the incident is over.

ACTION CHECKLIST

Counter-UAV Action Checklist

1. **Conduct a UAV threat assessment.** Identify likely launch areas, target points, high-value assets, approach routes, local threat actors, and whether drones are more likely to be used for surveillance, harassment, arson or attack.
2. **Map critical vulnerabilities.** Prioritise tank farms, fuel storage, loading gantries, control rooms, power generation, firefighting systems, valve stations, communications, accommodation and helipads.
3. **Establish government liaison before an incident.** Confirm who has legal authority to detect, track, jam, intercept or investigate UAVs. For high-risk operations, request police, military, civil aviation or national security support in advance.
4. **Develop a drone sighting protocol.** Include immediate reporting, alarm activation, control-room notification, incident logging, photography or video if safe, and escalation to authorities.
5. **Create site-specific response actions.** Define when to stop hot work, halt fuel transfer, isolate valves, move personnel to hardened shelter, suspend vehicle movement, or activate emergency response.
6. **Train guards and supervisors.** Security teams should understand drone indicators, common flight patterns, likely launch points, and what details to record. Training should include day and night scenarios.
7. **Drill the response.** Conduct tabletop and live drills for surveillance drone, loitering drone, explosive drone impact, fire at tank farm, secondary drone strike during firefighting, and drone debris recovery.
8. **Harden critical points.** Review protective options for firewater pumps, emergency generators, communication nodes, control rooms and exposed fuel systems. Prioritise consequence reduction over unrealistic total prevention.
9. **Build redundancy into emergency systems.** Firefighting systems should not rely on a single exposed pump, power source, hose route or control point. The Zawiya attack shows that firefighting infrastructure itself may be targeted.
10. **Control information.** Avoid posting site layouts, tank locations, guard routines, drone footage, emergency response movements, or live incident details on social media. Hostile actors can exploit this information.

11. **Preserve evidence safely.** If a drone crashes or debris is found, isolate the area, assume explosive hazard, prevent contamination, and hand the scene to authorised authorities.
12. **Review legal limits.** Confirm what the company can lawfully do in the operating country. Detection may be permitted; jamming, spoofing, interception or kinetic defeat may be restricted to state agencies.

OPERATIONAL IMPLICATIONS

Oil, Gas, Remote Operations and Critical Infrastructure

For oil and gas companies in Libya, the primary implication is that facilities can no longer treat UAVs as a military problem occurring somewhere else. Tank farms, power plants, pipeline nodes and port terminals are now realistic drone targets. The threat is especially serious where local militias, political factions or criminal groups are contesting control over infrastructure or revenue flows.

For remote operations, the most likely drone threat may initially be surveillance rather than attack. Drones may be used to observe camp layout, convoy departure times, guard routines, equipment storage, expatriate presence, or fuel points. However, surveillance can precede intimidation, sabotage or indirect attack. Remote operating sites should therefore include UAV reporting in daily security procedures, especially if operating near armed groups, disputed land, illegal mining zones, pipeline corridors or politically sensitive communities.

For critical infrastructure operators, the highest-value improvement is not necessarily buying expensive counter-drone systems. It is building a credible response system: detect early, protect people, reduce fuel and fire consequences, maintain communications, coordinate with government responders, and rehearse repeatedly. If national enforcement agencies can provide direct protection, mobile detection, airspace restrictions or response capability, that is the preferred option for high-risk periods.

FUTURE OUTLOOK

Outlook

Further violence around Zawiya remains possible. The drone strikes did not appear to be random; they targeted energy and power infrastructure in a city where armed political tensions are already high. If the Tripoli-based government increases pressure on Mohamed Bahroun or other local armed factions, further attacks against infrastructure, roads, depots, power facilities or security positions are plausible. The most likely near-term risk is not a nationwide escalation, but repeated localised attacks that disrupt energy supply and raise investor concern.

In eastern Libya, the killing of Maj. Gen. al-Mansouri may trigger an internal security response by the Libyan National Army. This could include arrests, checkpoints, intelligence sweeps, movement restrictions and heightened scrutiny of rival factions or suspected hostile networks in Benghazi. If the assassination is followed by further attacks against senior Libyan National Army figures, it would indicate a more serious penetration of eastern security structures.

For foreign companies, Libya remains commercially attractive but operationally fragile. The country's energy output has improved, and the National Oil Corporation continues to seek investment, but the security environment remains vulnerable to armed groups, local powerbrokers, drones, sabotage and targeted killings. Companies operating in oil and gas, logistics, construction, remote operations,

aviation and port services should treat UAV risk, local militia dynamics and emergency response resilience as central planning requirements.

The Zawiya incident should therefore be used as a trigger for practical review. Any company operating high-value infrastructure in Libya, or similar environments, should ask whether it could detect a drone before impact, protect emergency systems from a second strike, isolate fuel systems quickly, communicate with authorities, and run a rehearsed response without confusion. If the answer is no, the site is not ready for the current UAV threat environment.

SOURCE NOTE

Source Note

This report is based on reporting from Associated Press, Reuters, Libya's National Oil Corporation statements, and regional reporting. Source attribution has been limited within the body of the report to preserve analytical flow. Key referenced incidents include the 10-11 August 2026 UAV attacks against Zawiya refinery and power infrastructure, the National Oil Corporation emergency response, and the 10 August 2026 killing of Maj. Gen. Fawzy al-Mansouri in Benghazi.