Information Provided by Trident Group America, Inc

DRONES OVER THE RIG

Offshore Energy's Air Defense Gap and the Race to Fill It

THE SLEIPNER INCIDENT

A Documented Pattern of Unaddressed Incursions

- **1. On September 29, 2025,** an unidentified drone penetrated Equinor's Sleipner gas field complex in the North Sea.
- **2. Despite immediate detection,** no operator was identified, and no countermeasures were taken while the drone was present.
- **3. This incident follows a pattern since 2022,** with unauthorized drones reported at over ten oil and gas facilities.
- **4. The Sleipner breach highlights a critical reality:** offshore infrastructure is being surveilled with impunity.

HIGH-VALUE ATTACK SURFACE

The Strategic Concentration of North Sea Energy

- Norway is now Europe's largest natural gas supplier, making its offshore platforms a primary target for state-level pressure.
- A successful kinetic attack on a single major platform would trigger massive market shocks and energy supply disruptions.
- The North Sea also hosts over 100 offshore wind farms, representing an exponentially expanding and vulnerable attack surface.
- Protecting this distributed infrastructure across multiple national zones presents a security challenge with no onshore analogy.

THE JURISDICTIONAL VOID

Ambiguity in the Chain of Response Authority

01 Responsibility for counter-drone response offshore is significantly less clear than for onshore critical infrastructure.

02 Senior officials and industry leaders are still debating who is responsible for monitoring, escalating, and acting on incidents.

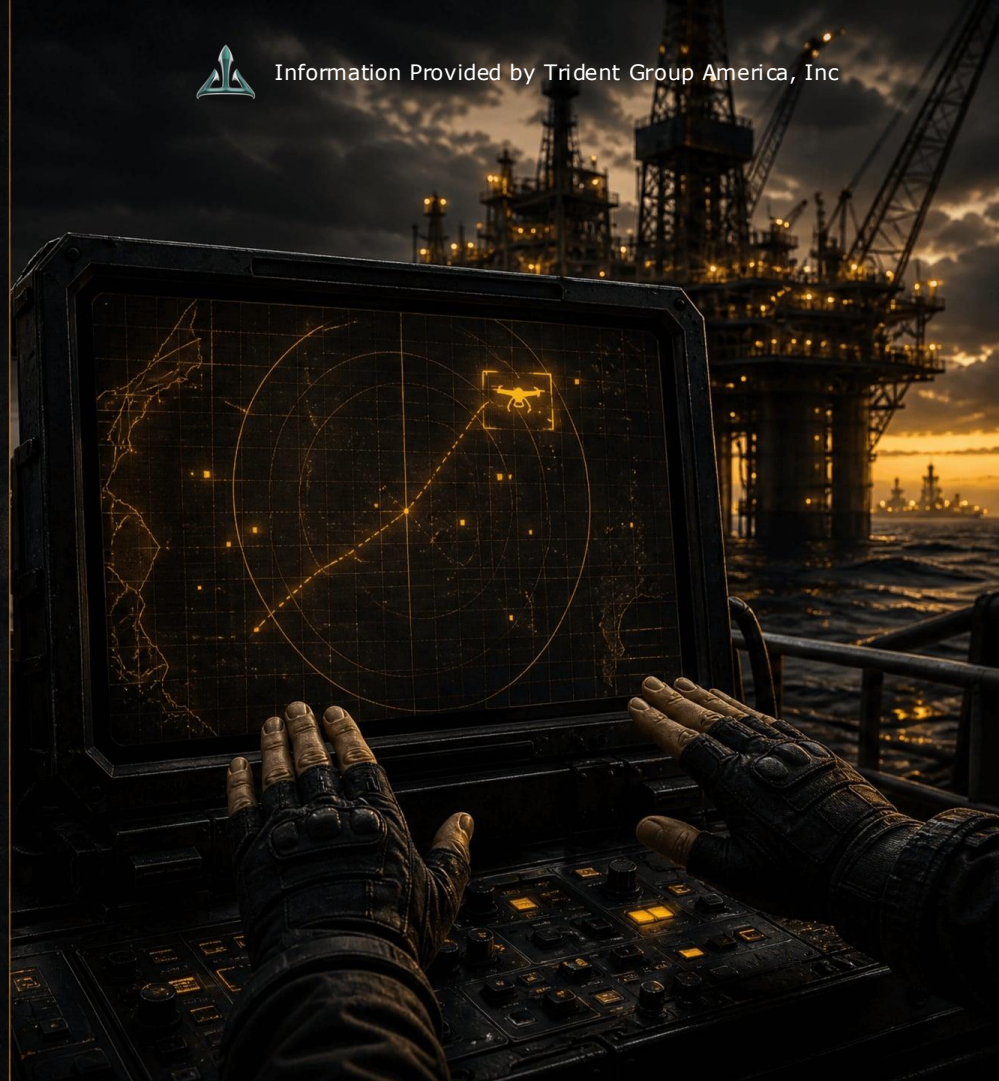
03 While entering a 500-meter safety zone is illegal, the operational capability to respond before a drone departs does not exist.

04 Shore-based response infrastructure cannot reach platforms hundreds of miles offshore within the critical time window.

THE PRIVATE SECURITY GAP

Detection Without the Legal Authority to Act

1. Operators have invested in radar and sensors capable of tracking unauthorized drones in their airspace.
2. However, private facility owners currently lack the legal authority to take any active countermeasures against detected drones.
3. Jamming or intercepting a drone can lead to aviation law violations, spectrum interference penalties, and criminal liability.
4. The constraint is not technical—it is a response authority gap that leaves operators as passive observers of their own risk.



THE SAFER SKIES ACT 2025

A Directional Shift in Counter-Drone Authority

1. Signed in December 2025, the Act expands federal authority to detect and mitigate credible drone threats to covered facilities.
2. It acknowledges that counter-drone response cannot be exclusively concentrated in a narrow club of federal agencies.
3. For the first time, U.S. law provides a pathway for state and local law enforcement to participate in drone mitigation.
4. While a significant step forward, the Act's implementing regulations are not due until mid-2026, leaving an interim gap.

Information Provided by Trident Group America, Inc

THE CERTIFICATION BOTTLENECK

The Massive Gap Between Policy and Operational Reality

1. The FBI's National Counter UAS Training Center is the sole certifying authority under the SAFER SKIES Act.
2. The center is projected to certify only 60 officers by June 2026, against demand from 18,500 law enforcement agencies.
3. Drone threats emerge and resolve in minutes, requiring a distributed response infrastructure that does not yet exist.
4. The certification pipeline is currently a planning framework, not a functional response infrastructure for critical assets.

Information Provided by Trident Group America, Inc

HYBRID ATTRIBUTION STRATEGY

Deliberate Ambiguity as an Operational Posture

1. Unattributed drone surveillance generates intelligence value without triggering the response threshold of an attributed state actor.
2. Actors are aware of monitoring deployments and confident in their ability to conduct operations within their limitations.
3. The pattern of unaddressed incidents normalizes surveillance and establishes the contours of detection and response capability.
4. A drone that surveys a platform without consequence provides tactical data on layout, personnel, and security positioning.

Information Provided by Trident Group America, Inc

THE VULNERABILITY PROFILE

Beyond Surveillance to Operational Disruption

1. Unauthorized incursions present risks ranging from surveillance to the potential delivery of kinetic payloads.
2. A single operator can complete a delivery or conduct surveillance before a coordinated response can be mounted.
3. Offshore platforms with volatile materials have a physical vulnerability profile different from onshore stadiums or prisons.
4. The inability to detect, track, and mitigate drones creates a window for catastrophic operational disruption.

THE INTERIM EXPOSURE

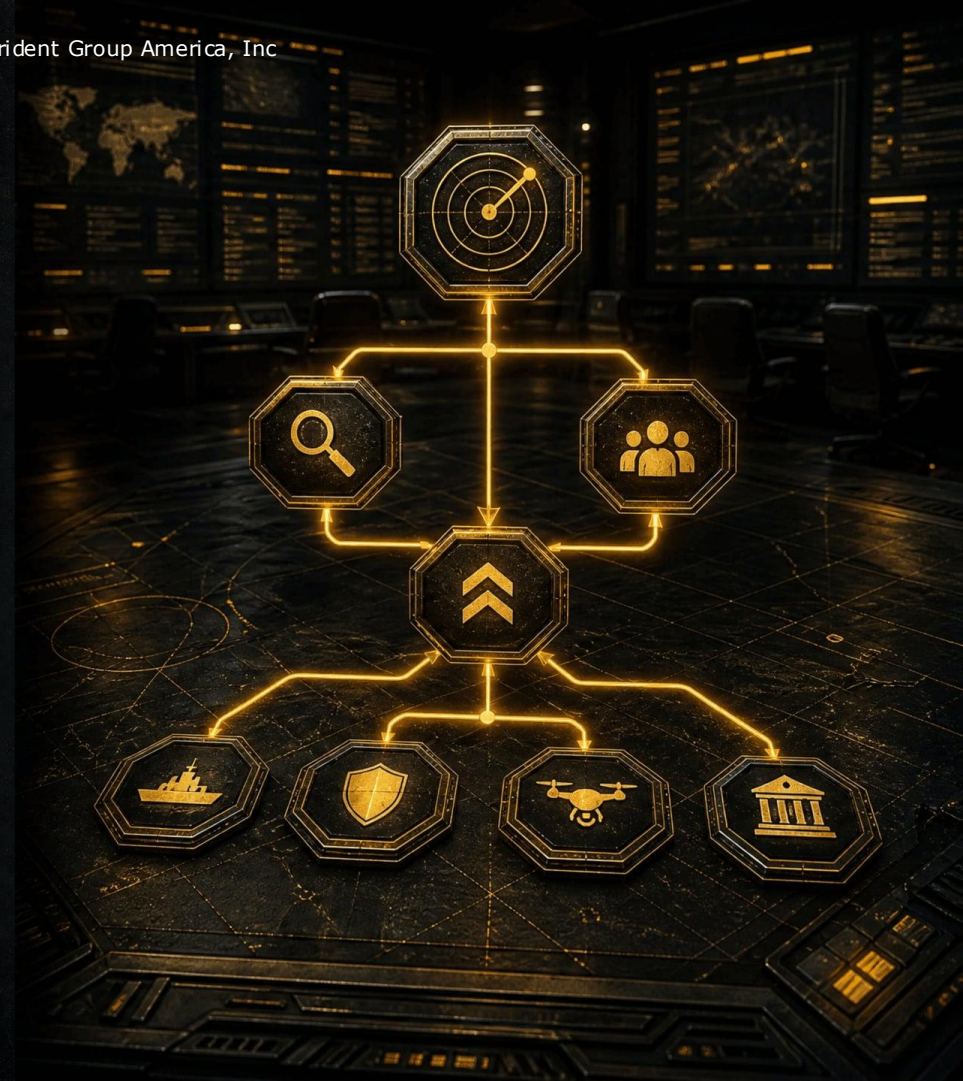
Navigating the Gap Before Full Implementation

1. The period between the Act's enactment and the 2026 regulations represents a high-risk window for operators.
2. Until regulations are published, state and local agencies cannot independently deploy the new mitigation authorities.
3. Operators must rely on existing, fragmented frameworks while the threat environment continues to evolve rapidly.
4. This interim period exposes the lag between legislative intent and the actual deployment of protective capabilities.

COORDINATED RESPONSE PROTOCOLS

Compressing the Decision-Making Window

1. Effective response requires pre-established communication protocols between operators, regulators, and naval authorities.
2. Defining the information that triggers each level of response is critical for meeting the narrow response window.
3. The UK model of security guidance between industry and government provides a structure for other jurisdictions.
4. Without clear escalation paths and authority chains, even the most advanced detection systems remain ineffective.



INTEGRATED SECURITY ASSESSMENTS

Bringing Airspace into the Facility Security Plan

1. Drone threat scenarios must be integrated into facility security assessments alongside physical and cyber frameworks.
2. Treating the airspace above the safety zone as "someone else's problem" is no longer a viable security posture.
3. ISPS Code compliance must evolve to account for the three-dimensional threat environment of modern offshore operations.
4. An integrated assessment is the foundation for building the detection and response capabilities the threat demands.

Information Provided by Trident Group America, Inc

CONCLUSION: THE UNPROTECTED AIRSPACE

Closing the Gap in Offshore Energy Security

1. Offshore energy infrastructure has become the most consequential unprotected airspace in the critical landscape.
2. The SAFER SKIES Act is a vital step, but its operational expression is years away from meeting the scale of need.
3. Closing the gap requires detection investment, coordinated protocols, and integrated security assessments.
4. The drones will not wait for the governance framework to catch up; the time for operational integration is now.

Information Provided by Trident Group America, Inc