TRIDENT GROUP
FROM KNOWLEDGE TO ACCESS TO SECURITY

DESIGNING FOR THE DRONE AGE

How Ukraine redrew the security spectrum for critical infrastructure and people — and why insurers and financiers have not yet caught up.

TRIDENT GROUP GLOBAL SECURITY OPERATIONS CENTER · JULY 2026

PREPARED FOR

Underwriters, IFIs & DFIs, Owners, Operators & Protective Principals

20×

MARITIME WAR-RISK REPRICING

Red Sea premiums: ~0.05% of hull value pre-crisis to ~1% at the 2024 peak — aerial threat has already repriced an insurance class

144

SUSPECTED DRONE SIGHTINGS, EUROPE

Across 13 European states + Ireland, Aug 2024–Feb 2026 (IISS) | half over military facilities

<10 → ~80

JNIM ARMED-DRONE STRIKES, 2024→2025

Sahel emulation of Ukraine-proven tactics | 2026 on pace to exceed 2025 (ACLED)

SECTION 01 — ASSESSMENT

EXECUTIVE SUMMARY

The war in Ukraine has done more than transform the military domain; it has redrawn the entire security spectrum. The lessons of mass, low-cost unmanned systems are no longer confined to front lines or to state armies. They have diffused — rapidly and deliberately — to terrorist organizations, transnational criminal organizations (TCOs), eco-extremist actors, nation-state proxies, and even individuals recruited online. For critical infrastructure — power generation, hydroelectric facilities, ports, data centers, and fuel farms — and for the protection of people — diplomats, corporate executives, and high-net-worth individuals — the implication is profound: **the threat now arrives from above, cheaply, and often without warning.**

COUNTER-UAS OPERATOR READIES A MULTIROTOR INTERCEPTOR PLATFORM

Insurance underwriters and international financial institutions (IFIs) have begun to scrutinize resilience more closely. In our assessment, however, **most underwriters, IFIs, and related stakeholders do not yet fully understand or appreciate how fundamentally the security baseline has shifted.** Closing that gap will require a comprehensive rethinking — and in many cases a physical re-engineering — of how facilities are designed, where critical functions are placed, and how people are protected.

IN THIS PAPER

SECTION 01 · CONTINUED
STRATEGIC ASSESSMENT

KEY JUDGMENTS

01

The threat environment has evolved faster than insurance models and financing criteria.

The deliberate, adaptive, aerial-attack threat to fixed infrastructure remains consistently under-weighted against climate, nat-cat, and cyber exposures.

02

Low-cost, high-volume drones have made critical infrastructure inherently more exposed.

An airframe costing a few hundred dollars can damage or destroy assets worth orders of magnitude more.

03

Resilience must be engineered upfront — not retrofitted under crisis conditions.

What is built into the ground or behind hardening at the design stage cannot be cheaply or fully replicated by a later retrofit.

04

Security-by-design is now a precondition for bankability and insurability.

A lack of insurability directly undermines bankability — the maritime market has already demonstrated the mechanism.

05

Human security, continuity, and governance are central to mission assurance.

Infrastructure is only as resilient as the people who operate, protect, and depend on it.

BOTTOM LINE

AN ASSET THAT CANNOT BE INSURED CANNOT BE FINANCED

Resilience omitted at the design stage cannot be recovered later at any reasonable cost. This white paper provides a framework for decision-makers to close that gap.

SECTION 02 — THREAT EVOLUTION

THE UKRAINE INFLECTION POINT

Ukraine has compressed a decade of unmanned-systems evolution into a few years: first-person-view (FPV) strike drones, fiber-optic control links that are immune to electronic jamming, long-range one-way attack drones, and integrated detection–electronic-warfare–interceptor architectures. **The decisive lesson is asymmetry.** An airframe costing a few hundred dollars can damage or destroy assets worth orders of magnitude more, and saturation tactics using cheap one-way attack drones expose the unsustainable cost asymmetry of conventional air defense.

Crucially, this is no longer a purely military phenomenon. The same capabilities are now relevant across the full security domain, including civilian critical infrastructure that planners once treated as rear-area and inherently safe. **A facility's distance from a front line no longer guarantees that it sits outside the threat envelope.**

DIMENSION	OLD ASSUMPTIONS	DRONE-AGE REALITIES
Time to Detect	Minutes to hours	**Seconds to minutes**
Cost to Attack	High (manned systems)	**Low (mass-produced drones)**
Reach	Tactical / regional	**Tactical to strategic**
Attribution	Clearer lines	**Disaggregated / ambiguous**
Infrastructure Risk	Perimeter-based	**Persistent / multi-vector**

ONE-WAY ATTACK DRONES STAGED FOR LAUNCH — PHOTO: ARMYINFORM

SECTION 03 — CAPITAL & RISK TRANSFER

THE INSURABILITY BLIND SPOT

CONSENSUS — 2026

"A lack of insurability directly undermines bankability — and resilience not engineered in early leaves assets uninsurable later in life."

— GLOBAL INFRASTRUCTURE FACILITY (G20), IFC, MIGA, AON, 2026

A consensus has consolidated in 2026 that insurability is becoming a precondition for bankability, and that resilience must be engineered into an asset during project preparation rather than retrofitted later.[1] Insurance capacity now materially affects bankability, loan requirements, and deal execution.[2] Yet the resilience conversation among underwriters and IFIs remains dominated by climate, natural-catastrophe, and cyber exposures. The deliberate, adaptive, aerial-attack threat to fixed infrastructure is consistently under-weighted.

The consequence is a latent mispricing. A power plant, port, fuel farm, or data center engineered to a pre-2022 security baseline may appear insurable today, yet drift toward being uninsurable — or insurable only at prohibitive cost — within its operating life. This is the same "uninsurable later in life" dynamic the GIF warns of, but driven by a deliberate and evolving threat rather than by weather. Through the first half of 2026 this has stopped being hypothetical: the incidents detailed in Section 4 have prompted explicit calls for critical-infrastructure operators to move on resilience now.[3] As with climate resilience, **the genuine window of influence is at design and preparation, not at retrofit.**

DRONE-AGE INSURABILITY MODEL

1 — THREAT ENVIRONMENT
Understand adversary capabilities, intent, and tactics.

›

2 — ASSET EXPOSURE
Identify critical assets, interdependencies, and vulnerability drivers.

›

3 — RESILIENCE DESIGN
Engineer layered defenses; detect, disrupt, and recover.

›

4 — BANKABILITY / INSURABILITY
Demonstrate resilience credible to insurers and financiers.

UNDERSTAND — DEMONSTRATE

WHY IT MATTERS

A security baseline set before 2022 can look insurable today and become uninsurable within an asset's operating life — the same dynamic the GIF warns of for climate, driven instead by a deliberate, adaptive adversary. The maritime precedent on the following page shows how quickly underwriters reprice once the threat becomes undeniable.

SECTION 03 · CONTINUED

THE MARITIME PRECEDENT

0.05% → ~1%
RED SEA WAR-RISK PREMIUM, % OF HULL VALUE, AT 2024 PEAK

40–60%
OF SUEZ CONTAINER TRAFFIC DIVERTED AROUND THE CAPE

+3,500 NM
AND 10–14 DAYS ADDED PER DIVERTED VOYAGE

The market has already repriced once — at sea. The proposition that aerial threat moves insurance markets is not a forecast; in the maritime domain it is an observed fact. The September 2019 drone and cruise-missile strike on Saudi Arabia's Abqaiq–Khurais complex took roughly 5.7 million barrels per day of processing capacity offline — about five percent of global supply — before the Ukraine war began.[13] Since late 2023, Houthi drone and missile attacks have repriced an entire insurance class: Red Sea war-risk premiums rose from a pre-crisis baseline of roughly 0.05% of hull value — often waived outright — to approximately 1% per seven-day transit at the 2024 peak, a twentyfold increase, while 40–60% of Suez container traffic diverted around the Cape of Good Hope.[14] Premiums stayed elevated even through the October 2025 ceasefire lull — Maersk waited two months before returning a single vessel — and in July 2026 a Houthi blockade declaration moved indicative rates from roughly 0.3% to 0.75% of vessel value within a single day, with the Strait of Hormuz simultaneously disrupted.[14] **What underwriters have already done to hulls, they will do to fixed infrastructure.** The only question is whether an asset's resilience posture is legible to them when they do.

The gap is worse than a pricing problem. For fixed assets, the sharper risk is not a higher premium but no recovery at all. Standard property and business-interruption policies commonly exclude damage from war, hostile acts, and terrorism; cover for deliberate attack typically lives in specialist political-violence and terrorism markets that many infrastructure owners have never bought, or have bought at limits set before the drone age. The attribution ambiguity described in Section 4 compounds the exposure: whether a strike is classified as war, terrorism, sabotage, or vandalism can determine which policy — if any — responds. An owner who has not mapped drone scenarios against actual policy wordings may discover at claim time that the asset was effectively self-insured against precisely this threat. Resilience engineering and coverage architecture must therefore be reviewed together, not in sequence.

SECTION 04 — PROLIFERATION

THE DEMOCRATIZATION OF THE DRONE THREAT

The proliferation and deployment of drones is not limited to militaries. It now includes terrorist groups, TCOs, eco-extremist actors, nation states, and even disgruntled insiders. Two dynamics make this durable: **a deliberate hybrid campaign by state actors, and rapid, documented emulation by non-state groups.**

Hybrid recruitment and escalation. Following the expulsion of its intelligence officers, Russia has become highly effective at online recruitment of third-country nationals to attack European critical infrastructure, using a deniable "gig-economy" model of disposable operatives.[4] The campaign has intensified into 2026: analysts have tracked more than 150 suspected Russia-linked hybrid incidents across the EU and NATO states tied to 2025 — a roughly fourfold year-on-year rise in sabotage and vandalism, with Germany alone reporting several hundred suspected incidents.[5]

A July 2026 IISS study reinforced the aerial dimension, plotting 144 suspected drone sightings across thirteen European states and Ireland between August 2024 and February 2026 — roughly half over military facilities and the remainder over civilian airports, ports, and energy infrastructure — and assessing that Russia highly likely launched some from shadow-fleet vessels offshore.[4] The campaign's most visible effects came in 2025, when drone incursions forced airport suspensions at Copenhagen, Munich, and Brussels.[6]

SECTION 04 · CONTINUED — PROLIFERATION

Through the first half of 2026 the aerial dimension has widened beyond deliberate hybrid operations: stray and electronically diverted drones from the long-range strike campaigns over Russia forced suspensions at Helsinki and Vilnius in May 2026 and ignited an oil-storage site in eastern Latvia — incidents that closed the airspace of NATO capitals, triggered the collapse of Latvia's governing coalition, and demonstrated that infrastructure now sits inside the threat envelope regardless of whether it is the intended target.[6] **Attribution ambiguity is itself part of the exposure.**

EMULATION IS EXPLICIT AND DOCUMENTED

HEZBOLLAH

LEVANT · FIBER-OPTIC FPV

Has openly drawn on the Ukraine war, fielding jam-resistant fiber-optic FPV drones flown up to roughly 20 km to strike Israeli armor with precision; in 2026 these drones have killed and wounded soldiers and were even launched at a medical-evacuation helicopter. Israeli analysts counted more than 80 explosive drones launched at IDF forces in the opening weeks of the April 2026 ceasefire alone, and attacks have persisted through its extensions and a June 2026 US-brokered framework agreement that Hezbollah has publicly rejected.[7]

LATAM CRIMINAL GROUPS

221 INCIDENTS · MEXICO 2021–25

Have industrialized weaponized drones — one study documented 221 incidents in Mexico from 2021–2025, 27 of them fatal with 77 killed — progressing to FPV, multi-munition release, and experimentation with fiber-optic control;[8] the pattern is spreading regionally, with Colombia recording its first lethal drone attack in 2024 and multiple drone deaths in 2025, and analysts reporting investigations into cartel operatives studying drone warfare in Ukraine.[9]

SAHEL JIHADISTS

JNIM · ISSP · AIRPORT ASSAULTS

JNIM and Islamic State Sahel Province escalated sharply: JNIM's armed-drone strikes rose from fewer than ten in 2024 to roughly eighty in 2025, with over 100 cases of drone violence recorded since 2023.[10] In 2026 the threat reached critical aviation infrastructure through complex assaults on the Niamey (January) and Tahoua (March) airports — the Niamey attack reportedly employing roughly ten kamikaze drones, the largest single-attack drone use by a Sahel-based militant group to date and a first for the Islamic State's Sahel Province in Niger, while the Tahoua raid deliberately targeted the state's own drone and ISR infrastructure. Niamey's airport was struck again by JNIM in June 2026. Allied groups were the first in the region to adopt the fiber-optic technique pioneered in Ukraine, and analysts expect 2026 to exceed 2025.[11]

The throughline is unambiguous: a capability set proven in Ukraine is being copied by state proxies, terrorists, and criminal organizations — and it will be emulated further. The barrier to entry has collapsed to a commercial drone, an online tutorial ecosystem, an improvised payload, and a willing operator. These threats will not only grow; they will be replicated across theaters and against new categories of target.

THE DRONE THREAT SPECTRUM

FPV DRONES	LOITERING MUNITIONS	ONE-WAY ATTACK UAVS	LONG-RANGE ISR / STRIKE
Short-range, high agility, low cost. Tactical precision against assets and personnel.	Persistent loiter, precision strike. Designed for infrastructure disruption.	Low-observable systems for stand-off strikes at scale.	Extended reach for ISR, targeting, and strategic effects.

SHORT RANGE / TACTICAL — LONG RANGE / STRATEGIC

SECTION 05 — BUILT ENVIRONMENT

RE-ENGINEERING THE BUILT ENVIRONMENT

The design assumption that the airspace immediately above a facility is benign no longer holds. Protecting critical infrastructure now demands that **overhead approach be treated as a primary attack vector from the earliest design stage.** Two principles follow.

PRINCIPLE 01

BURY OR HARDEN WHAT YOU CAN

Wherever feasible, critical and single-point-of-failure functions — control rooms, switchgear and transformers, fuel handling, SCADA and network cores, and sensitive data halls — should be placed below grade or within hardened, blast- and overhead-resistant structures. What is built into the ground or behind hardening at the design stage cannot be cheaply or fully replicated by a later retrofit.

PRINCIPLE 02

PROTECT IN LAYERS WHAT YOU CANNOT MOVE

Assets that cannot be buried or relocated — turbines, cooling plant, transmission yards, port cranes, and tank farms — require layered protection: standoff and redundancy, overhead screening and passive "cope cage"–type measures adapted from the battlefield, and, where lawful and feasible, an active layered defense that integrates detection, electronic warfare, and interception.

Measures that would have seemed unthinkable for civilian sites even two years ago are becoming a prudent design baseline. **Engineered in early, this is precisely the kind of resilience that underwriters and lenders reward; bolted on late, it is expensive and only partial.**

CRITICAL INFRASTRUCTURE IMPLICATIONS

ALL CRITICAL SECTORS FACE INCREASED EXPOSURE TO AERIAL AND CYBER-PHYSICAL THREATS

SECTOR	EXPOSED ASSETS & FUNCTIONS
Energy	Power generation and fuel storage; grid substations; pipeline and processing assets
Logistics	Ports and terminals; rail and road hubs; warehouses and distribution centers
Industrial Sites	Manufacturing plants; chemical facilities; utilities and water systems
Corporate Operations	Corporate campuses; data centers; executive travel and contingency
Insurance / Finance	Underwriting uncertainty; capital adequacy; credit risk and recovery scenarios

SECTION 06 — LEGAL & REGULATORY

THE LEGAL BOUNDARY OF COUNTER-UAS

No counter-UAS conversation with a civilian operator survives long before the legality question arrives, and it deserves a direct answer. **Detection, tracking, and identification** — radar, RF sensors, acoustic and electro-optical systems — are lawful in virtually every jurisdiction and should be treated as the universal baseline for any critical facility. **Active defeat is different:** jamming, spoofing, and kinetic interception remain reserved to state authorities in nearly all jurisdictions, and private actors who employ them face criminal exposure under communications, aviation, and computer-misuse statutes — in many legal systems a drone is an aircraft, and downing one is an offense regardless of intent.

SECTION 06 · CONTINUED — LEGAL & REGULATORY

The line, however, is moving. Ukraine's wartime practice has normalized layered civil-military airspace defense; NATO's "drone wall" initiative targets initial operational capability by the end of 2026; and national legislatures across Europe are expanding counter-UAS authorities for critical-infrastructure protection, while directives such as NIS2 raise the resilience obligations of the operators themselves.[15]

DESIGN IMPLICATION — THREEFOLD

Build **detection-first architectures** that are lawful everywhere today; concentrate investment in **passive measures** — hardening, standoff, screening, redundancy — which no statute restricts; and **pre-negotiate coordination** with the state authorities who hold active-defeat authority, so that the legal seam is bridged before an incident rather than during one.

SECTION 07 — PROTECTIVE OPERATIONS

PROTECTING PEOPLE, NOT JUST PERIMETERS

Security for diplomats, corporate executives, and high-net-worth individuals must be reconsidered on the same logic. Traditional close protection is optimized for ground-based threats — access control, perimeter security, motorcade discipline, and residential hardening. **The aerial vector inverts that model.**

Consider the now-credible scenario: an operator recruited online, equipped with an off-the-shelf commercial drone and an improvised payload, can threaten an executive who feels secure in a high-rise penthouse — while the protective team remains focused on building access and perimeter control far below. What was the stuff of science fiction only a few years ago is now an operational reality that VIP-protection teams must plan against.[12]

Effective personal protection now has to extend into the third dimension: airspace monitoring and detection, residence and venue selection that accounts for overhead lines of approach, and counter-UAS measures where legally permissible.

BEYOND ASSETS

THE HUMAN SECURITY DIMENSION

Infrastructure is only as resilient as the people who operate, protect, and depend on it. Human security includes physical safety, crisis communication, evacuation, leadership continuity, and organizational readiness. In the drone age, mobility, situational awareness, and governance are as critical as any physical barrier.

AIRSPACE AWARENESS IS NOW A STANDING REQUIREMENT OF PROTECTIVE OPERATIONS

SECTION 08 — MATURITY INSTRUMENT

THE DRONE-AGE RESILIENCE INDEX

A model becomes useful to underwriters and lenders only when it can be scored. The TGU Drone-Age Resilience Index (DRI) translates the four-step insurability model into a tiered maturity instrument that an insurer, IFI, or board can assess against — and that an owner can use to sequence capital allocation.

TIER	DESIGNATION	OBSERVABLE CRITERIA
0	**UNASSESSED** BELOW MODEL ENTRY	No aerial threat assessment; perimeter-based security model; airspace above the facility assumed benign; no detection capability.
1	**AWARE** DEMONSTRATES MODEL STEPS 1–2	Threat assessment current against adversary capabilities; critical assets and single points of failure mapped; aerial vectors incorporated into incident-response planning.
2	**MITIGATING** OPERATIONALIZES STEP 3	Persistent airspace detection and monitoring; passive protection applied to priority assets; continuity plans exercised; coordination channels with state authorities established.
3	**ENGINEERED** DELIVERS STEP 4 — BANKABLE	Security-by-design embedded at project preparation; critical functions below grade or hardened; layered detect–disrupt–recover architecture; resilience evidence packaged for underwriters and financiers.

TIER 0 · EXPOSED — TIER 3 · BANKABLE

READING THE INDEX

Tier progression tracks the insurability model directly: Tier 1 demonstrates Steps 1–2, Tier 2 operationalizes Step 3, and Tier 3 delivers the demonstrable, design-stage resilience that Step 4 requires — and the distance between Tier 1 and Tier 3 is precisely the latent mispricing described in Section 3.

TGU ASSESSMENT

MOST OPERATING INFRASTRUCTURE WORLDWIDE TODAY SITS AT TIER 0 OR TIER 1

SECTION 09 — RECOMMENDATIONS

IMPLICATIONS & A PATH FORWARD

Each recommendation below operationalizes a stage of the Drone-Age Insurability Model introduced in Section 3 — from threat understanding through demonstrated insurability — and the Drone-Age Resilience Index in Section 8 provides the instrument for measuring progression.

UNDERWRITERS & REINSURERS

MODEL STEPS 1 + 4

Incorporate deliberate aerial and hybrid-threat exposure into infrastructure underwriting, and treat hardened or below-grade design and counter-UAS provisions as risk-reducing investments rather than optional extras.

IFIS & DFIS

MODEL STEPS 2 + 4

Embed security-resilience criteria into project preparation and bankability assessment, alongside climate resilience — the same upstream stage where the most consequential decisions are locked in.

OWNERS, DEVELOPERS & OPERATORS

MODEL STEPS 2 + 3

Bring security engineering into the design phase, not procurement. The cheapest moment to harden an asset is on the drawing board.

PROTECTIVE-SECURITY PRINCIPALS

MODEL STEPS 1 + 3

Extend the protective bubble upward, and budget for airspace awareness as a standing requirement rather than an event-driven add-on.

STRATEGIC READ

THE ORGANIZATIONS THAT INTERNALIZE THIS FIRST WILL PRESERVE INSURABILITY, BANKABILITY, AND LIFE-SAFETY TOGETHER

The security baseline for critical infrastructure and for people has shifted faster than the institutions that finance, insure, and protect them have adjusted. Those that wait will discover the gap the hard way — and at a far higher price than design-stage resilience would ever have cost.

TGU ASSESSMENT — SIX HOLDINGS

- ✓ The security baseline has shifted permanently. Plan for a world where drones are ubiquitous.
- ✓ Resilience must be engineered from day one to preserve insurability and bankability.
- ✓ Layered detection, disruption, and hardening are essential across all critical sectors.
- ✓ Risk transfer solutions must evolve with the threat, backed by data and scenario modeling.
- ✓ People, governance, and continuity are decisive factors in mission assurance and recovery.
- ✓ Detection is lawful everywhere; active defense requires state partnership — bridge the legal seam before an incident, not during one.

ABOUT TRIDENT GROUP GLOBAL

Trident Group Global is a security, intelligence, and risk-advisory firm with a special-operations and maritime-security pedigree. Trident Group America, Inc. is incorporated in Florida, with its principal place of business in Virginia Beach, Virginia; Trident Group Ukraine operates a Global Security Operations Center (GSOC) in Kyiv. Focus areas include critical-infrastructure protection, maritime security, and counter-unmanned-aerial-systems (C-UAS) advisory and training.

SOURCES & REFERENCES

[1] Global Infrastructure Facility (GIF), Aon, IFC & MIGA, "Underwriting the Future of Resilience: Developing Insurable and Bankable Infrastructure" (white paper), March 2026.

[2] Aon, "Beyond Traditional Markets: Unlocking Alternative Risk Capital Solutions," 2026; and "Building Bankable, Resilient Data Centers: From Site to Operation," 2026.

[3] Aerotime, "Drone Threat to Europe's Critical Infrastructure Is Surging, Resilience Must Follow," May 2026.

[4] International Institute for Strategic Studies (IISS), "The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure," August 2025; RUSI, "Russian Sabotage in the Gig-Economy Era," 2024–2025; IISS drone-campaign dataset reported July 2026 (144 suspected sightings across 13 European states and Ireland, August 2024–February 2026; launches highly likely from shadow-fleet vessels).

[5] GL OBSEC & International Centre for Counter-Terrorism (ICCT), Russian hybrid-threat analysis cited in the Munich Security Report 2026; reporting on 150+ suspected EU/NATO incidents and a fourfold year-on-year rise, 2026.

[6] CEPA, "2026 — Europe's Year of Living Dangerously," December 2025 (Copenhagen, Munich, and Brussels airport closures, 2025); Reuters and Aerotime reporting, May 2026, and Sahaidachnyi Security Center Sub-Threshold Warfare Tracker (Helsinki and Vilnius suspensions, the Rēzekne oil-storage fire, and associated Latvian government fallout — incidents attributed to stray or electronically diverted drones from long-range strike campaigns over Russia, not to hybrid recruitment operations).

[7] The Times of Israel, June 2026; Al Jazeera and CNN, April–May 2026; Foundation for Defense of Democracies (FDD), May 2026 — on Hezbollah fiber-optic FPV drones adapted from the Ukraine war; Alma Research and Education Center, "Special Report: Hezbollah's FPV Explosive Drone Threat," May 2026 (80+ explosive drones launched at IDF forces since the April 18 ceasefire); Al Jazeera, June 2026 (Washington framework agreement and Hezbollah rejection).

[8] National Counterterrorism Innovation, Technology, and Education Center (NCITE), "Mapping Weaponized Drone Attacks Attributed to Mexican Drug Cartels, 2021–2025," 2026.

[9] CSIS, "Illicit Innovation: Latin America Is Not Prepared to Fight Criminal Drones," 2025 (incl. Colombia/ELN); Texas Public Radio / Defense News on cartel adaptation of Ukraine drone tactics, 2026.

[10] ACLED / DefenceWeb, "Jihadist Groups Pose a Growing and Expanding Threat in Africa," 2026 (JNIM strikes <10 in 2024 to ~80 in 2025; 100+ cases since 2023).

[11] ACLED expert comment on the 29 January 2026 Niamey airport attack (reported first ISSP use of an explosive-laden drone in Niger); Castorvali, "The Escalating Drone Threat in the Sahel and West Africa," March 2026 (approximately ten kamikaze drones at Niamey — the largest single-attack use by a Sahel-based group); Africa Defense Forum, April 2026 (fiber-optic adoption); regional reporting on the 8–9 March 2026 Tahoua Air Base 401 raid targeting drone infrastructure and the 18 June 2026 JNIM attack on Niamey airport.

[12] airsight, "Drones Present Threats to VIP Security and Privacy"; D-Fend Solutions, "Counter-Drone Solutions for VIP Protection," 2025.

[13] Reuters and International Energy Agency reporting on the 14 September 2019 Abqaiq–Khurais strike (approximately 5.7 million barrels per day of processing capacity offline; roughly 5% of global supply).

[14] Marsh McLennan war-risk pricing data cited by Insurance Business, June 2026 (~0.05% pre-crisis baseline to ~1% of hull value at the 2024 peak); Reuters, 20 July 2026 (indicative premiums from ~0.3% to ~0.75% following the Houthi blockade declaration); Verisk Maplecroft, 2025, and Forbes, July 2026 (Cape of Good Hope diversions and Suez traffic impact); BIMCO market guidance, February 2026 (Maersk return delay after the October 2025 ceasefire).

[15] AP / IISS reporting on the NATO "drone wall" initiative (initial operational capability targeted for end-2026), July 2026; EU Directive (EU) 2022/2555 (NIS2) resilience obligations for critical-infrastructure operators.

DOCUMENT CONTROL

REPORT ID	REVISION	PUBLICATION DATE
TGU-GSOC-WP-2026-0721-UA-01	**C**	**July 2026**
PREPARED BY	CLASSIFICATION	DISTRIBUTION
Trident Group Ukraine LLC · GSOC Kyiv	**UNCLASSIFIED // PUBLIC RELEASE**	**Approved for public release**

PRODUCED BY THE TGU GSOC

24/7 GLOBAL SECURITY OPERATIONS CENTER | KYIV

WASHINGTON DC

1500 K Street NW, Suite 200
Washington, DC 20005
+1-202-381-0361

KYIV

4 Mykola Hrinchenko Street
Kyiv 03038, Ukraine
+38-075-112-4078

REQUEST A SECURITY CONSULTATION

info@gotgu.co · tridentgroupukraine.com

SECURITY · RESILIENCE · CONTINUITY