

DRONE ATTACKS

ON COMMERCIAL
& INDUSTRIAL FACILITIES

Controlling Outcomes
Managing Liability
Protecting Assets

FOR OWNERS, SENIOR
EXECUTIVES, COMPANIES



BELSKIY
AND PARTNERS

FOREWORD

According to expert estimates, Russian businesses sustained approximately RUB 200 billion in losses from UAV attacks during the first half of 2026.

A UAV strike on an industrial, warehousing, or critical infrastructure facility, however, entails far more than physical damage and operational disruption.

It immediately exposes the business to multiple, parallel legal risk streams. At a minimum, these include the risk of insurance coverage being denied, disputes with counterparties arising from disrupted contractual performance, and heightened scrutiny by law enforcement and regulatory authorities.

Experience consistently demonstrates that the ultimate financial and legal consequences of a UAV strike are determined not only by the severity of the incident itself, but by the quality of the company's initial response.

The most consequential factors during the critical early stage include the timely notification of insurers and contractual counterparties, comprehensive preservation of evidence documenting the attack and its consequences, the availability of complete documentation relating to the affected asset, and a consistent legal position across criminal, insurance, and contractual matters.

For management, therefore, the principal issue extends well beyond the amount of physical damage sustained. The decisive questions are how the incident is officially documented, what evidence is preserved before it is lost, and how effectively the company's legal response is coordinated from the outset.

We have analyzed court decisions together with an extensive body of investigative practice relating to UAV attacks from 2024 through 2026. The same recurring patterns emerge with remarkable consistency across virtually every matter.

This Alert sets out a practical, end-to-end framework for managing legal risk before, during, and after an aerial attack, including attacks involving UAVs, missiles, and other aerial weapons. Properly implemented, this framework helps preserve insurance coverage, strengthen the company's litigation and regulatory posture, and materially reduce legal and commercial exposure for both the business and its management.

CONTENTS

1. Foreword	2
2. Critical Legal Risks Following a UAV Attack	4
3. Criminal Law Classification: Why It Matters	5
4. Force Majeure Following a UAV Attack: Judicial Treatment	7
5. Insurance Recovery: Coverage Limitations and Response Strategy	9
6. The First 24 Hours After a UAV Attack: Establishing the Company's Legal Position	10
7. Critical Errors That Weaken Legal Position	12
8. Engagement Of External Counsel: When To Retain	12
9. Executive-Level Strategic Guidance	13

CRITICAL LEGAL RISKS FOLLOWING A UAV ATTACK

The chart below maps the principal legal and business risks triggered by a UAV attack. The risks are organized by legal and commercial category to illustrate not only their source, but also their practical consequences for the company. Depending on how the incident is managed, these consequences may include denial of insurance coverage, contractual liability, prolonged operational disruption, increased regulatory and law enforcement scrutiny, and significant management and compliance costs.

RISK AREA	RISK LEVEL	BASIS FOR LIABILITY	LEGAL AND FINANCIAL OUTCOME
Criminal	High	The victim cannot determine the legal qualification. Investigative authorities have exclusive discretion to classify the conduct, including as terrorism (Art. 205), sabotage (Art. 281), property damage (Art. 167), murder (Art. 105), or other offenses under the Criminal Code.	Misclassification creates a material coverage risk. Early inaction may forfeit control of the factual record and determine the outcome of subsequent disputes.
Insurance	Critical	Standard insurance policies generally exclude losses caused by military UAV attacks. Coverage often depends on a Terrorism/Sabotage endorsement, available only upon legal classification of the incident under Articles 205 or 281 of the Criminal Code.	Complete denial of insurance coverage resulting from an incorrect criminal classification. Even where coverage applies, recovery may be substantially limited by a mandatory deductible and an aggregate sublimit capping the insurer's total liability for all claims arising from the insured peril.
Civil	High	Force majeure outcomes are fact-specific. Courts may reject defenses absent proof of exceptional circumstances, direct causation, and a complete evidentiary record. Commercial operators face a heightened burden of proof.	Liability for breach of contract, including damages and other contractual remedies. Without contemporaneous and properly documented evidence, reliance on a force majeure defense is unlikely to withstand judicial scrutiny.
Operational	Moderate-to-High	Damage to hazardous industrial facilities and critical energy infrastructure, leading to production shutdowns and supply chain disruption.	Prolonged operational downtime, termination of mission-critical commercial contracts, erosion of key business relationships, and loss of investor confidence.

While each of these risk categories presents a distinct source of exposure, the most significant threat to the Company arises when they converge. For that reason, these risks should not be evaluated as discrete issues. They are properly understood as an integrated risk architecture in which developments in one area directly shape the Company's overall exposure.

This framework demonstrates that the consequences of a UAV attack are determined less by the incident itself than by the Company's legal and operational readiness before the incident occurs. The critical variables are the breadth and allocation of insurance coverage, the contractual allocation of risk, the integrity of contemporaneous documentation, and the effectiveness of internal response protocols.

CRIMINAL LAW CLASSIFICATION: WHY IT MATTERS

The criminal law classification of an incident is the investigating officer's formal determination of the offense committed and, accordingly, the statutory provision of the Criminal Code under which criminal proceedings will be initiated.

In this category of disputes, classification is not merely descriptive—it is outcome-determinative. It defines the legal framework within which insurers assess coverage, counterparties evaluate force majeure defenses, and the company's engagement with law enforcement is ultimately conducted.

In practice, attacks against hazardous industrial facilities ("HIFs") and critical energy infrastructure—including power plants, oil depots, and fuel storage facilities—are typically classified as terrorist acts under Article 205 of the Criminal Code of the Russian Federation. By contrast, attacks targeting residential properties and other non-industrial assets are treated far less consistently, with investigators frequently relying on provisions such as Articles 167 (property damage) or 105 (murder). Most such cases never proceed to trial on the merits and remain at the pre-trial investigation stage. As a result, the investigating officer's initial classification is rarely subjected to meaningful judicial scrutiny and, as a practical matter, becomes the controlling legal characterization for every subsequent proceeding.

From a commercial perspective, this distinction is critical. Where an incident is classified under Articles 167 or 105 rather than Articles 205 (terrorism) or 281 (sabotage), insurance recovery under Terrorism/Sabotage coverage is, in most cases, effectively foreclosed regardless of the magnitude of the loss. The classification decision therefore extends well beyond the criminal process: it directly affects the company's ability to preserve and recover the economic value of its claim.

Accordingly, a business affected by a UAV attack cannot afford to remain a passive observer while awaiting investigative decisions. The company should instead take an active role from the outset in ensuring that the investigative record contains the factual and legal evidence necessary to support the legally correct classification of the incident. This includes evidence concerning the nature of the facility, its designation as a hazardous industrial facility or critical energy infrastructure, its economic or strategic importance, the apparent objective of the attack, and the gravity of its consequences.

The procedural tools available to advance that objective include:

- filing a criminal complaint setting out the proposed legal classification of the offense;
- submitting motions requesting specific investigative measures and seeking reclassification of the offense pursuant to Articles 119, 122, and 159 of the Criminal Procedure Code of the Russian Federation;
- challenging investigative decisions before the head of the investigating authority or the prosecutor under Article 124 of the Criminal Procedure Code; and
- seeking judicial review of investigative decisions under Article 125 of the Criminal Procedure Code.

Petitions addressed to the Business Ombudsman, relevant ministries, the State Duma, the Federation Council, or the Presidential Administration may, in appropriate cases, serve as an additional source of external institutional pressure and can at times prove effective. They are, however, no substitute for the core procedural work of building the evidentiary record within the criminal case itself.

The single most effective practical tool is the company's own parallel internal investigation, conducted by its legal department, security function, and external counsel alongside the official criminal investigation. Its purpose is not to replicate the work of law enforcement but to identify, preserve, verify, and promptly place into the investigative record evidence bearing directly on the legal classification of the incident. Such evidence includes the facility's technical and regulatory status, the nature and extent of the damage, the scale of the resulting consequences, documentation relating to anti-terrorism security compliance, records establishing the facility's operational and technological function, and any other material capable of influencing the legal characterization of the attack.

FORCE MAJEURE FOLLOWING A UAV ATTACK: JUDICIAL TREATMENT

Unmanned aerial vehicle ("UAV") attacks may disrupt manufacturing operations and supply chains, requiring businesses to promptly notify counterparties and address the resulting inability to deliver products or perform contractual obligations on time.

As a result, disputes increasingly center on whether a party may be excused from liability for non-performance or delayed performance by invoking a UAV attack as a force majeure event.

Russian case law addressing whether UAV attacks constitute force majeure has been developing since 2024. As of June 2026, the jurisprudence remains fragmented and, at times, inconsistent, with no authoritative guidance from the higher courts.

The analytical framework continues to be the well-established three-part test articulated by the Plenum of the Supreme Court of the Russian Federation in Resolution No. 7 dated March 24, 2016. A party invoking force majeure must independently establish each of the following elements:

- **Extraordinary Nature** — the event was exceptional under the specific circumstances.
- **Unavoidability** — the event could not reasonably have been prevented despite the exercise of due care and all reasonable preventive measures.
- **Causation** — the UAV attack directly caused the inability to perform the specific contractual obligation at issue.

From a litigation perspective, each element must be proven independently. Failure to establish any one of them will ordinarily defeat a force majeure defense.

Regional Approach Remains Outcome-Determinative

Region	Prevailing Judicial Approach
Donetsk People's Republic (DPR), Luhansk People's Republic (LPR), Kursk Region, Belgorod Region	Force majeure generally rejected. Courts increasingly view recurring UAV attacks as a foreseeable commercial risk rather than an extraordinary event.
Tver Region, Samara Region, Ulyanovsk Region, Rostov Region, and others.	Force majeure more readily recognized where supported by a robust evidentiary record demonstrating the required legal elements.

Courts apply **a more demanding standard to professional operators** such as warehouse operators, logistics providers, and carriers.

A generalized reference to wartime conditions or elevated security risks is insufficient. Instead, the defendant is generally expected to demonstrate that it implemented every reasonable risk-mitigation measure available under the circumstances, including, where appropriate:

- deployment of available protective systems or security measures;
- procurement of terrorism-risk insurance;
- prompt notification of contractual counterparties.

Courts typically expect a comprehensive evidentiary record, which may include:

- a force majeure certificate or opinion issued by the regional Chamber of Commerce and Industry or the Chamber of Commerce and Industry of the Russian Federation;
- official communications from competent military authorities, the Federal Security Service (FSB), or the National Guard (Rosgvardiya);
- a resolution initiating a criminal investigation;
- independent expert reports documenting property damage;
- records issued by EMERCOM, including emergency declarations or counterterrorism operation orders, where applicable; and
- photographic and video evidence documenting the consequences of the attack.

That evidence, however, is not dispositive. Documentary proof cannot substitute for the critical element of causation. The party invoking force majeure must still demonstrate that the UAV attack directly prevented performance of the particular contractual obligation within the required timeframe.

Accordingly, disputes of this nature frequently evolve into an examination of the company's pre-incident risk management rather than a debate over the attack itself.

Courts assess not only the external event but also whether the defendant was reasonably prepared for such a contingency, how promptly it notified its counterparty, what concrete steps it took to mitigate the consequences, and whether the evidentiary record establishes a direct causal nexus between the UAV attack and the specific contractual breach.

Ultimately, these cases rarely turn on whether a UAV attack may qualify, in the abstract, as a force majeure event. The dispositive question is whether the party invoking the defense has established—based on the particular facts—that the event was extraordinary, objectively unavoidable despite reasonable diligence, and the direct cause of its inability to perform the contractual obligation at issue.

In practice, therefore, the outcome is driven as much by contractual risk allocation, contemporaneous documentation, timely notice, and the overall quality of the evidentiary record as by the underlying incident itself.

INSURANCE RECOVERY: COVERAGE LIMITATIONS AND RESPONSE STRATEGY

Whether losses resulting from a UAV attack are recoverable under an insurance policy depends first and foremost on the policy wording—not on the mere existence of insurance coverage. Standard commercial property policies typically provide only limited protection against such losses. Although many policies are issued on an “all risks” basis, coverage for UAV-related damage is commonly narrowed by broad exclusions, while any potential recovery is often conditioned on the satisfaction of additional coverage triggers.

Typical Exclusions Under Standard “All Risks” Policies:

- the use, impact, or crash of military UAVs, including resulting debris;
- the operation of air-defense systems and damage caused by falling interceptor missiles or their components; and
- the impact of missiles, projectiles, munitions, or related fragments of any kind.

In practice, recovery frequently depends on a dedicated “Terrorism” and “Sabotage” endorsement. Importantly, such coverage is not triggered automatically. Coverage typically becomes available only if the underlying incident is formally classified by the investigative authorities as terrorism (Article 205 of the Russian Criminal Code) or sabotage (Article 281 of the Russian Criminal Code). Accordingly, the availability of insurance proceeds may ultimately depend on the legal characterization adopted during the criminal investigation. From a practical standpoint, this makes the insured’s timely and effective engagement with the investigative process a critical component of any insurance recovery strategy.

Key Insurance Policy Provisions to Review

Policy Provision	Key Considerations
Terrorism/Sabotage Sublimit.	Confirm the sublimit and whether it applies per insured or on an aggregate basis. Separate sublimits provide broader protection.
Deductible	Assess deductible exposure. Lower or conditional deductibles provide broader coverage.
Multiple Attacks Within a Six-Hour Period.	Verify whether multiple incidents constitute a single occurrence. Single-occurrence treatment generally maximizes recovery.
Contingent Business Interruption Coverage.	Confirm coverage for supply-chain losses arising from terrorism or sabotage. The absence of such an exclusion materially strengthens coverage.

To maximize recoverability, policyholders should seek to:

- extend coverage to UAV-related damage regardless of the criminal-law classification ultimately assigned to the incident;
- replace an unconditional deductible with a conditional deductible;
- establish separate sublimits for each insured within a corporate group, where applicable; and
- structure those sublimits on a per-occurrence basis rather than as an aggregate limit applicable to multiple successive events.

Ultimately, insurance disputes arising from UAV attacks are rarely resolved by the mere existence of an insurance policy. Instead, the outcome is driven by the legal architecture of the policy itself.

As a practical matter, recovery typically turns on the convergence of three factors: (i) the legal classification assigned to the incident by the competent authorities, (ii) the scope and structure of the policy's coverage, and (iii) the extent to which the policy was negotiated and tailored to address the insured's actual operational risk profile before the loss occurred.

THE FIRST 24 HOURS AFTER A UAV ATTACK: ESTABLISHING THE COMPANY'S LEGAL POSITION

The first 24 hours following a UAV attack constitute a critical phase in establishing the evidentiary record and preserving procedural leverage. During this period, the initial factual record is created, contemporaneous documentation is generated, and the foundational legal characterization of the incident is established. That initial framing will subsequently influence criminal proceedings, insurance coverage determinations, regulatory reviews, and contractual disputes.

At this stage, the issue is not the ultimate outcome of future proceedings, but rather the range of legal positions that will remain available. The facts that become accepted as established, the documents admitted into the evidentiary record, and the notices deemed legally sufficient are largely determined during this initial response period. Errors made within the first 24 hours frequently become structural weaknesses in the company's legal position and may be difficult — if not impossible — to cure at a later stage.

This is the point at which three critical legal positions are formed simultaneously:

- the criminal-law characterization of the incident;
- the insurance coverage position; and
- the contractual and force majeure position vis-à-vis counterparties.

The initial evidentiary record is established, legally sufficient notice procedures are initiated, and key factual circumstances are preserved for use in all subsequent proceedings and negotiations. Accordingly, legal oversight of the incident — including the immediate engagement of counsel experienced in insurance coverage disputes, criminal investigations, and complex commercial litigation — must begin at the moment of initial response, not after a dispute has already materialized.

IMMEDIATE LEGAL PRIORITIES FOLLOWING A UAV ATTACK



Control of the Criminal-Law Characterization of the Incident

- Promptly notify investigative authorities, emphasizing the facility's strategic, hazardous production facility status, and/or critical fuel and energy infrastructure status.
- Immediately assert potential offenses under Articles 205 (Terrorism) and/or 281 (Sabotage) of the Criminal Code, where supported by the facts.
- Submit documentation confirming the facility's classification, including its anti-terrorism protection and regulated infrastructure status.



Immediate Notice to the Insurer

- Promptly notify the insurer of potential terrorism and/or sabotage coverage, where applicable.
- Document the notice, including the date, time, delivery method, and recipient.



Force Majeure Notices to Contractual Counterparties

- Issue force majeure notices within the applicable contractual notice period (ordinarily three days).
- Failure to provide timely notice is, by itself, sufficient to preclude reliance on a force majeure defense.



Preservation of Evidence and Litigation Hold Measures

- CCTV footage, access-control records, and sensor data.
- operational logs, maintenance records, and technical documentation.
- photographs and video recordings of the damage area before any repair, cleanup, or remediation activities commence.



Immediate Engagement of Legal Counsel

- control the scope and substance of information provided to investigative authorities.
- prevent premature or legally disadvantageous characterization of the incident.
- coordinate a unified legal strategy across three parallel tracks: investigative authorities; insurers; and contractual counterparties.

CRITICAL ERRORS THAT WEAKEN LEGAL POSITION

ERROR	LEGAL CONSEQUENCE
Failure to proactively influence the criminal-law characterization of the incident.	Adverse criminal classification may trigger policy exclusions and result in denial of insurance coverage.
Failure to provide timely force majeure notice to counterparties.	Loss of contractual force majeure protections and potential judicial rejection of the defense.
Reliance on generic force majeure language without establishing causation.	Exposure to liability for contractual non-performance.
Failure to provide documentation confirming the hazardous production facility status / fuel and energy infrastructure status.	Loss of critical leverage in seeking recognition of terrorism-related classification under Article 205 of the Criminal Code of the Russian Federation.
Commencing repairs or cleanup before completing formal documentation of damage.	Irreversible loss of evidence necessary to support subsequent claims and disputes.
Absence of pre-existing facility documentation and compliance records.	Inability to promptly provide required evidence to investigative authorities and insurers.

ENGAGEMENT OF EXTERNAL COUNSEL: WHEN TO RETAIN

Retain external counsel with expertise in insurance coverage and criminal defense at the following stages:

- **Immediately after the UAV attack** — to influence the legal characterization of the incident during the pre-investigation inquiry.
- **Upon first contact with law enforcement** — before providing any statements or explanations.
- **When responding to insurer inquiries** regarding the characterization of the incident.
- Upon receipt of claims from counterparties alleging contractual breaches.
- If the investigative authorities adopt an adverse legal characterization — **to challenge that determination through available legal remedies.**

EXECUTIVE-LEVEL STRATEGIC GUIDANCE

Drone attacks require more than an effective operational response. They demand a risk-management framework established well before an incident occurs.

Management's responsibility is to ensure that four critical components are in place: (i) a coordinated engagement strategy with law enforcement authorities; (ii) a contractual framework that preserves the ability to invoke force majeure when warranted; (iii) insurance coverage aligned with the facility's actual risk profile; and (iv) organizational and documentary preparedness capable of supporting the Company's legal and insurance positions immediately following an incident.

From a criminal-law perspective, management's objective is to ensure that the factual record and supporting evidence permit the incident to be characterized under legal provisions that both accurately reflect the asset's significance to the business and preserve available insurance coverage, rather than leaving the legal characterization entirely to investigative authorities. Achieving that objective requires established internal protocols, predefined escalation procedures, and the institutional capability to conduct an independent factual investigation from the outset.

Contractually, the priority is to create conditions under which force majeure can be asserted—and substantiated—in practice, rather than existing only as boilerplate language. That requires disciplined notice procedures, deliberate allocation of contractual risk, and transaction-specific drafting that accounts for regional operating conditions and foreseeable security risks.

From an insurance standpoint, the critical question is whether the insurance program actually responds to the facility's exposure profile, taking into account the legal characterization of the event, applicable sublimits, deductibles, exclusions, and limitations on consequential losses. That determination is ultimately a management decision—not the insurer's. Insurance should therefore be evaluated as an integral component of the Company's enterprise risk and financial strategy, rather than as a compliance exercise or a procurement formality.

Ultimately, the Company's documentary and organizational readiness, including complete supporting records, current internal protocols, clearly assigned responsibilities, and decision-making authority established in advance, will largely determine the effectiveness of its legal and insurance strategy after an incident. Without that foundation, even the strongest litigation team and the most carefully negotiated insurance program will be materially constrained in protecting the Company's interests.