The 2026 Iran War, Tax Audits, and Force Majeure: The UAE Supreme Court's Standard for Force Majeure in Tax Audits and Liabilities

March 2, 2026

The outbreak of the Iran War on 28 February 2026 has abruptly plunged the Middle East into profound operational disruption. Consequently, corporate boards operating within the United Arab Emirates are instinctively looking to the doctrine of *force majeure* and emergency circumstances (*thuroof tari'a*) as legal shields. Having acted in over 300 UAE tax dispute procedures, one of the most pressing questions we are now receiving is whether the friction of Iran War legally diminish underlying tax liabilities, excuse administrative penalties, or suspend Federal Tax Authority (FTA) audit procedures.

To answer this purely as a matter of law, we must detach from the immediate fog of conflict and examine the definitive jurisprudence of the UAE Federal Supreme Court. The seminal judgment in Cassation No. 958 of 2025 (Administrative) provides the exact legal architecture. In that dispute, the systemic crisis in question was the COVID-19 pandemic. By transposing the Court's rationale regarding the pandemic onto the 2026 conflict, we find a resolute and unyielding framework of administrative tax law.

The Statutory Accrual of Tax Liability

A question taxpayers make during wartime is whether the disruption of their administrative capabilities lawfully

postpones their underlying tax liabilities. The Supreme Court systematically dismantled this assumption, establishing that the legal character of a tax debt operates entirely independently of the operational environment.

The Court ruled that tax obligations are rigidly attached to the statutory transaction date, irrespective of the taxpayer's ability to seamlessly file declarations during a crisis:

"The legislator did not make the acquisition of the status of 'payable tax' contingent upon the tax return, but rather bestowed this status upon the tax whose payment date has arrived."

Therefore, as far as matters stand, the geopolitical landscape does not alter the realization of a statutory tax point. Even if the Iran War prevents the timely filing of an administrative return, the underlying liability is not practically paused or legally dissolved. The war does not suspend statutory accrual.

Force Majeure: Transposing Covid-19 to the 2026 Conflict

During the COVID-19 pandemic, taxpayers attempted to utilize the global emergency as a *force majeure* event to excuse administrative delays, avoid late penalties, and invalidate tax assessments. In the petition for Cassation No. 958 of 2025, the UAE Federal Supreme Court considered *force majeure* in regard to tax audits. They highlighted a three-year audit delay, noting that the FTA itself admitted its operations were hindered by COVID-19.

In light of the legal maxim that "a party cannot benefit from its own mistake" the Supreme Court considered whether the FTA could not lawfully impose incremental "time-based penalties" while the government's own pandemic-related disruptions stalled the audit process. Furthermore, the Supreme Court considered whether the FTA's crisis-induced delay caused a compensable "loss of opportunity" to mitigate penalties under

favorable Cabinet Decisions issued to provide relief during the pandemic.

Today, businesses are considering whether this exact legal theory would apply to the 2026 Iran War, and whether regional hostilities inherently frustrate audit procedures, trigger mutual *force majeure* exemptions, and legally dissolve the imposition of administrative fines.

The Federal Supreme Court, however, addressed the premise that a systemic crisis suspends tax obligations or shifts the legal burden. Addressing the attempt to use the pandemic to excuse compliance failures, the Supreme Court laid down a formidable standard that directly governs our current wartime reality:

"…its admission of its …-month delay places the burden of proof upon it despite the Corona pandemic that passed over everyone (the Appellant and the Administrative Authority)."

The Rationale: Crises That "Pass Over Everyone"

The jurisprudential rationale here is profound. Because a systemic crisis, whether a global health emergency like COVID-19 or the 2026 Iran War, impacts both the private sector and the state apparatus equally, its mere existence does not grant the taxpayer blanket legal immunity.

The fact that the crisis "passed over everyone" means the foundational rules of administrative litigation remain intact. The Court made it clear that a shared macroeconomic shock does not reverse the burden of proof:

"The burden of proof in an administrative dispute does not deviate in its origin, and as a general rule, from others, as the principle is that the creditor must prove the obligation and the debtor must prove getting rid of it…"

Taxpayers cannot use general claims of *force majeure* as a shield against statutory tax audits or potential government

disruptions. To successfully challenge an FTA assessment during this conflict, general appeals to wartime hardship are legally insufficient; taxpayers must rely on pristine documentary evidence demonstrating exactly how the war rendered specific compliance materially impossible.

Conclusion

Does the 2026 Iran War diminish or dissolve UAE tax liabilities or audit procedures? The unequivocal legal answer from the UAE Supreme Court is not in a blanket manner. Guided by the rationale in Cassation No. 958 of 2025, the judiciary does not recognize systemic, shared crises as a *force majeure* that extinguishes tax debts or shifts the burden of proof. The machinery of UAE tax law does not halt for war. Taxpayers whose tax audits or liabilities are affected by the war must provide direct evidence, grounds, and standing to causation and nexus in approaching the FTA, the tax disputes resolution committees, or the courts.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

UAE Crypto Litigation: The "Man in the Middle" and the Duty of Delivery

March 2, 2026

The following is an excerpted analysis of topics discussed in

the book UAE Crypto Litigation, a treatise on the judicial evolution of digital asset disputes in the United Arab Emirates, available at www.uaecryptolitigation.com.

A defining feature of blockchain transactions is their irreversibility. If an asset is sent to the wrong address, there is no central authority to reverse the transaction. This technical reality creates complex legal questions when a transaction is intercepted or misdirected by a malicious third party; a "Man in the Middle" attack. In China, the US, and the UK, courts have often placed strict liability on OTC desks to verify the identity of the recipient. The UAE courts, applying general principles of contract law, have allocated this risk strictly against the seller in the context of delivery obligations.

The Dubai Court of Appeal recently analysed a dispute arising from a Peer-to-Peer (P2P) sale of USDT. The buyer had paid for the assets, and the seller transferred the USDT to a wallet address provided by a third-party intermediary who was facilitating the deal. The intermediary, upon verifying the transfer, vanished with access to that wallet, leaving the buyer empty-handed.

The court held the seller liable for the buyer's loss. It established a high standard for the duty of delivery, ruling that the obligation to deliver sold goods is not met by merely dispatching them to a provided address. The seller must ensure the successful *receipt* of the assets into the buyer's effective control. By relying on an untrusted intermediary's instructions without verifying the wallet's ownership with the buyer directly, the seller assumed the risk of fraud.

This judgment reinforces the "perfect tender" rule in the context of digital assets. It serves as a caution to OTC traders who rely on brokers on platforms like Telegram. The legal duty is result-oriented: the contract is only performed when the buyer has the tokens, not when the seller has sent

them. If the intermediary provides a fraudulent address, the party sending the funds bears the loss.

To navigate the risks of P2P transactions and intermediary liability, see more in 'UAE Crypto Litigation' book publication available at www.uaecryptolitigation.com.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

War Series: The 1991 Gulf War UNCC Precedent and the Arbitration of Environmental Damage in Conflict Zones

March 2, 2026

When Iraqi forces retreated from Kuwait in 1991, they left behind an unprecedented ecological catastrophe. Over 600 oil wells were set ablaze, and millions of barrels of crude oil were intentionally released into the Persian Gulf. The sky turned black, and coastal ecosystems were devastated. Beyond the profound human and structural toll of the conflict, the international community was faced with a novel legal dilemma: How do you quantify, litigate, and arbitrate the destruction of an ecosystem in the aftermath of war?

The answer came in the form of the United Nations Compensation Commission (UNCC), a quasi-judicial, mass-claims body

established by UN Security Council Resolution 687. The UNCC's handling of environmental damage claims, specifically its "F4" claims category, laid the foundational precedent for how international law and modern arbitral tribunals approach the financial liability of environmental destruction in war zones.

As contemporary conflicts in regions like Eastern Europe and the Middle East result in the destruction of dams, the targeting of chemical plants, and the scorching of agricultural land, the legacy of the UNCC remains a critical framework for states, international investors, and corporations navigating post-conflict arbitration.

The F4 Claims: Quantifying the Unquantifiable

Before the 1990s, international legal mechanisms for addressing war reparations heavily favored property damage, lost profits, and personal injury. The environment was often viewed as a silent, uncompensable casualty of armed conflict.

The UNCC revolutionized this by formally recognizing claims for "environmental damage and the depletion of natural resources." The "F4" claims category allowed governments to seek compensation not just for the loss of commercially viable resources (like oil), but for the restoration of ecosystems.

Crucially, the UNCC established that compensation could be awarded for:

- **Preventative measures:** The costs of mitigating further environmental degradation.
- **Reasonable restoration:** The expenses associated with cleaning up shorelines, remediating soil, and extinguishing oil well fires.
- **Monitoring and Assessment:** Funding to study the long-term health and ecological impacts, acknowledging that environmental damage often takes years to fully manifest.

The Commission ultimately awarded over $5.2 billion for environmental remediation and restoration, setting a towering precedent that pure ecological harm—distinct from commercial loss—has quantifiable legal standing.

From the UNCC to Modern Arbitration

While the UNCC was a specialized commission rather than a traditional commercial arbitration tribunal, its methodological framework deeply influences modern international dispute resolution. Today, when environmental disasters occur during armed conflicts, the legal mechanisms have shifted primarily toward investor-state dispute settlement (ISDS) under Bilateral Investment Treaties (BITs) and commercial arbitration.

1. The Valuation of Ecological Harm

When an international energy or mining company's assets are caught in a war zone, the resulting environmental spillover often violates host-state environmental regulations. If a host state attempts to penalize a foreign investor for war-induced environmental damage, tribunals frequently look to the UNCC's rigorous evidentiary standards. The UNCC established that claimants must prove a direct causal link between the military action and the specific environmental harm, preventing opportunistic claims.

2. Force Majeure and Environmental Liability

For multinational corporations operating in conflict zones, environmental destruction often triggers complex *force majeure* disputes. If a facility is bombed and toxic chemicals leak, who is responsible for the cleanup? Traditional contracts may excuse the failure to deliver goods during a war, but they rarely absolve a company of overarching environmental liabilities. The UNCC precedent underscores that the entity responsible for the military aggression ultimately bears the financial burden of the ecological fallout, a principle

routinely debated in modern force majeure arbitrations.

3. The Rise of “Ecocide” in International Discourse

The precedents set in the early 1990s are currently being tested by the realities of modern warfare. With the destruction of critical infrastructure increasing in modern conflicts, legal scholars and arbitrators are increasingly engaging with the concept of “ecocide.” As states and corporations prepare to arbitrate the massive costs of post-war reconstruction, the UNCC’s formula for valuing the restoration of water tables, agricultural land, and biodiversity will serve as the starting point for tribunals.

Business Considerations for the Modern Era

For businesses and investors operating in politically volatile or conflict-prone regions, the integration of environmental risk into dispute resolution strategies is no longer optional. The UNCC precedent teaches us that environmental damage in war is not legally “collateral.” It is a highly scrutinized, financially quantifiable liability.

Companies must ensure that their investment contracts and insurance policies explicitly define environmental liability in the event of armed conflict, recognizing that international tribunals now possess the historical precedents and economic methodologies to hold parties accountable for the earth they scorch.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

UAE Crypto Litigation: Specific Performance and the Return of the Asset In Specie

March 2, 2026

The following is an excerpted analysis of topics discussed in the book UAE Crypto Litigation, a treatise on the judicial evolution of digital asset disputes in the United Arab Emirates, available at www.uaecryptolitigation.com.

When a debtor defaults on a loan of 10 Bitcoin, or an employer fails to pay a salary denominated in tokens, what is the appropriate remedy? In the United States, the bankruptcy proceedings of entities like *Celsius* and *FTX* have famously "dollarized" claims as of the petition date, often locking creditors into losses at the bottom of the market. The UAE courts, however, are increasingly adopting a property-law approach that favors *specific performance,* ordering the return of the asset itself, rather than its fiat equivalent.

This shift is evident in a landmark decision by the Dubai Court of First Instance regarding a private loan of 16 Bitcoin. When the borrower defaulted, the court did not engage in a complex valuation exercise to convert the Bitcoin to Dirhams; a process fraught with difficulty given the asset's intraday volatility. Instead, it ordered the defendant to return 16 Bitcoin *in specie* to the claimant. This implicitly recognizes the digital asset not merely as a value-reference, but as a distinct class of property capable of direct restitution, akin to the specific delivery of chattels in English law.

This principle has even extended to employment disputes. In a novel judgment, a Dubai court ordered an employer to pay

outstanding wages in “Ecowatt tokens,” as strictly stipulated in the employment contract. By enforcing the delivery of the specific token, the court upheld the sanctity of the contract’s currency clause.

However, judicial pragmatism dictates a fallback position. Where the specific asset cannot be returned, such as in cases of fraud where the tokens have been dissipated, the Dubai Court of Cassation has established a critical valuation rule. Monetary compensation must be calculated based on the market value at the time of the *judgment*, not the time of the breach. This forward-looking valuation ensures that a fraudster cannot profit from the market’s appreciation during the delays of litigation, ensuring the victim is made economically whole in current terms.

To understand the strategic implications of seeking specific performance versus monetary damages, see more in ‘UAE Crypto Litigation’ book publication available at www.uaecryptolitigation.com.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Musk Announces SpaceX to Build Self-Growing City on the Moon Within 10 Years

March 2, 2026

It is not unbeknown to the public that NASA, for over a decade now, has been working to get humans back on the Moon. This has been a long and challenging journey that has successfully culminated in the Artemis II launch to the Moon this year. On the other side of the aisle, SpaceX and Musk have publicly stood ground on their desire to push the journey just a few kilometers further to Mars instead. However, on 8 February 2026, via X (formerly, Twitter), Musk announced:

"[…] SpaceX has already shifted focus to building a self-growing city on the Moon, as we can potentially achieve that in less than 10 years, whereas Mars would take 20+ years […] That said, SpaceX will also strive to build a Mars city and begin doing so in about 5 to 7 years, but the overriding priority is securing the future of civilization and the Moon is faster."

(emphasis added)

The phrasing matters. Musk did not describe a "base," a "camp," or even a "permanent presence." He chose "self-growing city" a term that, in space systems language, implies a settlement that can expand its own capacity faster than Earth can sustain it through resupply. In other words, the decisive milestone is poised to be the point at which the city can manufacture, repair, and reproduce the core inputs of life and industry on-site, with Earth shifting from a lifeline to a partner.

This emphasis on speed is also crucial. In the expanded announcement, Musk explicitly contrasted lunar cadence with Martian cadence because the former provides frequent launch opportunities and short transit times allowing rapid iteration, while Mars imposes long windows between optimal departures and months-long transfers. The Moon, in Musk's framing, is simply the faster pathway to the larger objective, reducing the risk that a disruption on Earth can strand an off-world population before it is self-sufficient.

What a “self-growing city” would actually mean

A credible “self-growing” settlement is less a single project than a layered stack of capabilities that compound over time.

First, a survivable envelope or atmosphere. A city would begin with pressurized volume, radiation protection, thermal control, and redundancy. On the Moon that likely means habitats that are either buried, barriered, or shielded with regolith. Engineering for sustained occupancy is necessary to turn temporary infrastructure into long-term habitat.

Second, reliable power at city scale. Early lunar outposts can run on solar with storage; a city that grows needs power that is both scalable and resilient through lunar night, dust, and operational contingencies. That can mean distributed solar fields, large-scale storage, and, notably, nuclear surface power (see more on the plans for this here). The commercial point is that power becomes the first utility market of the lunar economy, and everything else prices off it.

Third, closed-loop life support and food production. “Self-growing” implies that water, oxygen, and consumables are not flown in as a permanent operating model. A settlement can still import specialty components, medicines, and high-value electronics but it cannot depend indefinitely on routine shipments of basic life inputs without remaining fragile by design.

Fourth, industrial metabolism by extraction, processing, and manufacturing. This is where “city” plays a critical role in an envisioned lunar economy. A lunar settlement that grows must be able to produce increasing quantities of:

- structural materials (regolith-based bricks, sintered surfaces, composites),
- spare parts and tools (additive manufacturing),
- propellants and volatiles if polar ice is exploited, and
- replacement infrastructure (power hardware, pressure

shells, mobility platforms).

In practical terms, “self-growing” means establishing an industrial base: each new machine, habitat module, or power unit increases the settlement’s ability to build the next one.

Fifth, governance by logistics. A lunar city will function as a managed system: inventory control, redundancy planning, maintenance cycles, and emergency protocols will be as central as rockets. The romantic imagery of flags and footprints matters less than the operational question of whether the settlement can survive a sustained interruption of Earth resupply.

Why the Moon becomes strategically attractive

Musk’s core argument is speed. The Moon is close enough to allow rapid learning cycles (launch, land, test, fix, repeat) on timelines that resemble industrial development rather than expeditionary exploration.

That matters because establishment of a large-scale settlement will not be a single “mission.” It will be an accumulation of failures and successes: life support anomalies, dust mitigation, thermal shock, power reliability, human factors, medical contingencies. A two-day transit and frequent windows change the economics of failure.

It also matters because NASA’s own lunar return effort remains on a near-term timetable. As of early February 2026, NASA indicated Artemis II is targeting no earlier than March 2026 following issues identified during a fueling test. Against that backdrop, a public SpaceX narrative that the Moon is the near-term priority signals an alignment with where the most immediate institutional demand sits.

What this shift means for the industry

If SpaceX truly prioritizes a lunar city three effects follow

across the market.

1) The lunar economy becomes real and fast.
A city implies persistent demand for cargo, construction, power, comms, navigation, mobility, and surface operations. That demand creates bankable markets for companies that are not launch providers: mining and excavation, robotics, thermal systems, pressure vessel manufacturing, radiation shielding, surface mobility, and autonomous operations.

2) “Cislunar logistics” becomes the main arena of competition.
A high-value advantage of establishing a lunar settlement is cadence. Any actor that can move mass routinely will set the tempo for everyone else. Musk’s own commentary places “millions of tons” and scale at the center of the ambition. The competitive response will not only come from rival launch systems, but from anyone building cislunar transportation, depots, tugs, and surface freight capacity.

3) Regulation, liability, and contract standards will tighten.
A city forces the legal questions to mature. Risk will address launch and reentry, but expand to long-duration habitation, industrial activity, and sustained operations in proximity to other actors. That pushes regulators and contracting authorities toward stricter requirements on safety cases, mission assurance, spectrum discipline, debris and traffic coordination, and insurance coverage tailored to continuous lunar operations.

It also changes the commercial posture of space law. The legal work shifts towards operational governance rather than mission approval: how activity is coordinated, how safety zones are treated in practice, how responsibility is allocated across operators and contractors, and how disputes are resolved when operations become continuous rather than episodic.

Conclusion

This is not a retreat from Mars so much as a recalibration of

sequencing. Musk still describes Mars as a continuing objective, with work beginning in the five-to-seven-year range, but with the Moon as the overriding priority because it is faster.

If the Moon becomes the proving ground for genuine self-sufficiency via energy independence, industrial reproduction, and survivable logistics, then the lunar decade will be the architectural foundation for everything that follows.

So that means that we are all heading to the Moon, SpaceX included.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

UAE Crypto Litigation: WhatsApp and the Unsigned Contract

March 2, 2026

The following is an excerpted analysis of topics discussed in the book UAE Crypto Litigation, a treatise on the judicial evolution of digital asset disputes in the United Arab Emirates, available at www.uaecryptolitigation.com.

In the fast-paced environment of crypto-trading, formal contracts are frequently neglected in favor of instant messaging. Deals worth millions are struck via WhatsApp, Telegram, or WeChat, often with little more than a “thumbs up”

emoji to signify assent. When these informal arrangements collapse, the UAE courts are tasked with a forensic inquiry: can a string of text messages constitute a binding commercial contract? The answer, as revealed by recent appellate judgments, depends entirely on the content of the messages and the value of the claim.

The UAE approach offers an interesting parallel to the “parol evidence rule” in US contract law or the statutory requirements for writing in the UK’s Law of Property (Miscellaneous Provisions) Act. Generally, the UAE Law of Evidence requires written proof for obligations exceeding a certain value. However, the courts have adapted to the digital age by accepting electronic correspondence as a “commencement of proof in writing,” provided it is sufficiently clear.

In a striking example of this flexibility, the Dubai Court of First Instance enforced a multi-million dollar liability based almost exclusively on WhatsApp messages. While the initial oral agreement was unprovable, the defendant’s subsequent messages, in which he explicitly acknowledged the debt and promised repayment, were treated as a binding extra-judicial admission. Here, the informality of the medium did not negate the clarity of the confession.

However, there is a limit to this indulgence. The Abu Dhabi Court of Appeal recently drew a hard line in a case involving an alleged five-million-dollar investment. The claimant attempted to reconstruct complex contractual terms from a series of WhatsApp exchanges. The court dismissed the claim, finding that while messages can prove a debt, they are often too fragmented and ambiguous to establish the nuanced terms of a partnership or a high-value investment mandate. Unlike the Chinese courts, which have developed specific protocols for verifying blockchain and WeChat evidence, the UAE courts apply a traditional lens to new media: if the messages do not clearly define the “meeting of minds” on all essential terms, they cannot substitute for a formal contract.

Furthermore, the courts are wary of "unsigned contracts" circulated via email. In another Dubai case, a claimant relied on an unsigned draft contract and screenshots. The court dismissed the claim, reinforcing that an unexecuted document has no evidentiary value unless corroborated by decisive conduct or admissions. The message to the market is clear: while digital chat logs can save a claim by proving an admission of debt, they are a poor substitute for a signed agreement when trying to prove the complex terms of a venture.

For a practical guide on preserving digital evidence and understanding its weight in court, see more in the evidentiary chapters of 'UAE Crypto Litigation' book publication available at www.uaecryptolitigation.com.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Russian Spy Satellites Intercepting European Satellite Communications

March 2, 2026

European space security officials are increasingly concerned that two Russian "inspector" satellites have been used to collect communications associated with multiple European satellites, including traffic linked to government and military users. This has evidently been a sustained pattern over several years, with the alleged consequence being

intelligence collection and a clearer mapping of how European satellite services could be constrained or disrupted in crisis conditions.

Such activity risks compromising sensitive information transmitted by the satellites but could also allow manipulation of the satellite flight paths or even lead to accidents.

What is reported to have happened

The reporting attributes the assessment to European security and intelligence officials who have been tracking two Russian spacecraft commonly referred to as Luch-1 and Luch-2. Officials reportedly believe these spacecraft were able to intercept communications from at least a dozen European satellites. The reporting also notes close approaches to a wider set of satellites over a multi-year period, which, if accurate, would reflect deliberate station-keeping near targets rather than incidental co-location in geostationary orbit.

A key technical qualifier is that interception risk is not uniform. A close look points to legacy vulnerabilities, including the fact that some older satellites may still rely on weak or unencrypted command links, creating exposure not only for confidentiality but also for command authentication and operational integrity.

None of this requires assuming a “weapon” in orbit. Persistent proximity operations, combined with modern signals-intelligence payloads, can be sufficient to collect metadata, waveform characteristics, traffic volumes, and in some cases content, depending on encryption and link discipline. Even where encryption holds, the collector learns usage patterns, the contours of the ground segment, and system behavior under stress.

Why proximity operations matter commercially

Geostationary orbit is a commercial operating environment. Many satellites carry mixed traffic of commercial connectivity, leased capacity, and governmental payloads or services. That makes “space security” inseparable from commercial service continuity and contract performance.

Three immediate consequences follow.

First, security standards will move from guidance to gating. Encryption, authenticated command and telemetry, and disciplined key management are no longer features that win competitive bids. They are baseline conditions for eligibility, particularly for government and critical-infrastructure customers.

Second, underwriting and financing will harden around cyber-physical risk. The market already prices launch and debris risk. Persistent proximity and interception concerns introduce a more political category: contested-domain operating risk. That tends to produce tighter warranties, more onerous security representations, and narrower coverage around interference events.

Third, customers will demand assurance, not only service levels. Expect procurement language to expand beyond uptime and throughput into incident response timelines, sovereign control of command chains, ground segment resilience, and demonstrable ability to maintain service under interference conditions.

These pressures are intensified by Europe’s parallel policy direction toward sovereign secure connectivity. In January 2026, public statements from the European Commission described the commencement of GOVSATCOM operations, explicitly framed as secure and encrypted governmental satellite communications under European control.

The legal consequences: duties exist, but enforcement is political

The legal framework for outer space has not suddenly become obsolete. It is, however, strained by conduct that sits *below* the threshold of overt attack while still producing strategic harm.

Under the Outer Space Treaty, States must conduct activities with “due regard” to the corresponding interests of other States, and where a State has reason to believe an activity would cause “potentially harmful interference,” it should undertake appropriate international consultations. This is not a direct prohibition on collection, and it does not neatly capture intelligence operations. It does, however, create a lawful diplomatic pathway: if proximity operations are credibly framed as creating a risk of harmful interference or unsafe behavior, consultations are the treaty-based mechanism to press the issue.

Separately, Article VI’s responsibility principle matters in today’s mixed government-commercial architecture: States bear international responsibility for national activities in outer space, including those by non-governmental entities, and must authorize and continuously supervise such activities. In practical terms, this pushes European regulators toward more explicit security supervision of licensed operators whose systems carry government traffic, and it strengthens the policy case for security conditions in licensing and procurement.

The radio layer adds another legal and regulatory vocabulary. The International Telecommunication Union radio regime is designed to prevent harmful interference and imposes obligations on administrations regarding stations under their responsibility. If interception evolves into jamming, spoofing, or service disruption, that framework provides process and terminology even when remedies remain political.

The limiting factor across these regimes is attribution and proof. Legal consequences scale with confidence. That reality

will drive investment in independent tracking, data fusion, and evidentiary discipline, because sustaining a position in a diplomatic, regulatory, or legal forum matters.

Strategic meaning: below-threshold pressure becomes normal

The most consequential implication is not that satellites can be listened to. It is that space is being treated as a continuously contested domain, and that this contest is increasingly conducted through activity that stays below the threshold of overt interference.

For operators, the lesson is straightforward: resilience must be engineered and contractually demonstrated.

For governments, the implication is equally clear: the line between commercial service and national capability is thin, and it will continue to thin. Hybrid payloads, shared capacity, and multi-use constellations bring efficiency, but they also bring shared exposure.

For Europe, this incident reporting will likely accelerate three tracks already underway: (1) hardening of legacy systems and uplink security practices; (2) procurement and licensing reforms that make security a condition of market access; and (3) sovereign and allied connectivity architectures that reduce single points of failure and impose higher security baselines.

The diplomatic posture should remain measured. The objective is to reduce strategic ambiguity, raise the cost of intrusive behavior through collective standards and coordinated responses, and ensure that Europe’s commercial satellite market remains credible to the customers who depend on it.

In short, the future will not be defined by a single episode of proximity collection. It will be defined by whether Europe treats this as an intelligence curiosity, or as a governance and market-structure inflection point.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

The Private Sector's Increasing Control on National Security

March 2, 2026

For much of the last century, national security was treated as a sovereign stack: intelligence, armed forces, and state-controlled strategic infrastructure. The private sector mattered, but mainly as a supplier.

That separation is thinning across the world. In a period defined by gray-zone pressure, cyber disruption, and sustained geopolitical competition, private firms increasingly operate the systems that keep states functional under stress. They design the networks that move data, the platforms that process it, the factories that scale production, and the services that can be surged in crisis.

This is not a story about governments outsourcing security; states still carry legal authority, coercive power, and strategic responsibility. It is a story about where operational leverage now sits.

Critical Infrastructure and the "Public Risk"

The modern economy runs on privately owned and operated infrastructure that is strategically exposed. Undersea

telecommunications cables, which carry the overwhelming majority of transoceanic digital communications, are owned and operated by private companies and consortia. This reality is now being treated as a geopolitical fact, not a technical footnote.

In the **United Kingdom**, this has led to the recognition of the "private ownership of public risk." Under the National Security and Investment (NSI) Act, the UK government now scrutinizes private acquisitions across 17 sensitive sectors, including AI and energy, treating commercial activity as a core national security vulnerability. Even the UK's nuclear deterrent relies on private firms like Lockheed Martin for maintenance, proving that sovereign capabilities are deeply integrated with private industry.

Similarly, in **Europe**, the NIS2 Directive expands cybersecurity obligations to thousands of private organizations. By making these firms legally responsible for risk management and incident reporting, the EU effectively treats the private sector as the frontline of the "sovereign stack".

The Industrial Base as a Security Instrument

Security competition has returned to a basic question: can capacity be produced fast enough, at scale, and under constraint? This question implicates private industry first. Multi-state security groups now emphasize the need to aggregate demand and use longer-term orders to accelerate industrial capacity.

Australia provides a leading example of building "sovereign capabilities" through private partnerships. To support the AUKUS security partnership, Australia is leaning on private innovation in robotics and quantum technologies. Strategic mergers, such as the Australian firm Penten with the UK-based Amiosec, are now seen as essential to creating global providers of digital security for the state.

Space: A Case Study in Strategic Speed

Space illustrates how commercial services become strategic infrastructure in months, not decades. In recent conflicts, commercial satellite connectivity and sensing became operational necessities. This has triggered a shift in how states like **Canada** view their "digital ambition." Canadian analysts are increasingly arguing for the modernization of the "sovereign stack" by better integrating private-sector cloud and AI solutions, moving away from rigid, state-only classification frameworks.

Analysis: Future Control and the Security Arithmetic

As we look toward the future, the private sector is fundamentally changing the state's "security arithmetic". Private firms do not carry sovereignty, but they carry strategic consequence, creating four recurring dilemmas:

1. **Rule-Setting:** Who sets the rules for access or technical restrictions when private services are used in conflict?
2. **Concentration Risk:** How do states avoid single points of commercial failure without destroying the economics of the private market?
3. **Cross-Border Friction:** How do global firms reconcile operations with sanctions and competing alliance expectations?
4. **Resilience Contracting:** How do governments contract for resilience and "surge capacity" rather than just peacetime performance?

The future of national security will be defined by "dual-use" infrastructure, private runways, ports, and subsea cables that serve both commercial and military purposes. Intelligence is being redefined as private companies become part of "epistemic communities" integrated into state networks due to their specialized data analytics.

A mature approach treats the private sector as a standing

component of national security planning. This requires pre-negotiated surge mechanisms, routine exercises that include industry as an operational partner, and the construction of the legal and technical scaffolding necessary to make private capability reliable when the pressure spikes. In a world of persistent competition, the decisive question is no longer just what the state can do, but how effectively it can command the private leverage it no longer directly owns.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

China Unveils Five-Year Space Strategy: Behind What Beijing is Building and Why it Matters

March 2, 2026

On 29 January 2026, China formally unveiled its next five-year roadmap for its space sector. Led by the China Aerospace Science and Technology Corporation ("CASC"), the plan sets out a coordinated national strategy spanning space tourism, orbital digital infrastructure, satellite megaconstellations, deep-space exploration, and space resource development.

Unlike earlier plans that focused primarily on launch capability and national missions, this roadmap is explicitly commercial. It reflects Beijing's shift from building space

access toward designing a full space economy, integrating transportation, data, communications, computing, and long-term off-Earth operations into a single industrial system.

Below is what China is planning over the next five years and what it means for operators, investors, and governments.

Space Tourism as a Regulated Market

China placed space tourism directly inside its national development framework, committing to achieve operational suborbital tourism within the five-year window, followed by a phased transition toward orbital passenger services.

This matters more for what it enables structurally. Human-rated vehicles drive reusable launch systems, crew safety standards, insurance markets, ground infrastructure, and regulatory frameworks for commercial human spaceflight. By incorporating tourism into state planning, China is signaling that these enabling layers will be built in parallel.

Several Chinese startups are already developing suborbital vehicles, but CASC's endorsement elevates tourism from speculative private activity to state-supported industry. The practical outcome will likely be accelerated certification pathways, coordinated launch infrastructure, and easier access to capital. In effect, tourism becomes the catalyst for a broader commercial ecosystem.

For international operators, this introduces a new state-backed competitor in a market previously dominated by Western firms.

Space-Based Computing and AI

The most strategically significant element of the announcement is China's commitment to develop space-based digital infrastructure, including orbital data processing and AI platforms.

These systems envision satellites performing compute-intensive tasks directly in orbit, forming a space-based cloud layer powered by continuous solar exposure and unconstrained by terrestrial energy grids. Rather than downlinking raw data to Earth for processing, China aims to analyze imagery, communications, and sensor outputs in space before transmitting refined products to ground users.

This architecture reshapes the economics of Earth observation, secure communications, autonomous navigation, and defense-adjacent analytics. It also introduces sovereign digital environments beyond traditional jurisdictional boundaries.

Western companies have discussed similar concepts, including SpaceX through its broader constellation strategy, but China is now embedding orbital computing directly into national industrial planning. Over the next five years, this is likely to drive large-scale satellite deployment, new spectrum requirements, and accelerated development of space-qualified processors and networking systems.

For regulators and operators alike, orbital computing raises unresolved issues around cybersecurity, liability, data governance, and congestion management.

Deep Space Capability and Talent Development

China is also expanding its deep space ambitions. Just days before the announcement, the University of the Chinese Academy of Sciences launched a School of Space Exploration focused on advanced propulsion, trajectory modeling, and long-range mission design.

This move institutionalizes deep-space expertise inside China’s technical pipeline, ensuring a steady flow of engineers trained for lunar operations, autonomous spacecraft, and eventual interplanetary missions. The five-year plan frames the coming decade as a window for leapfrog development in deep-space technologies, linking talent cultivation

directly to national exploration objectives.

Practically, this supports sustained lunar activity, robotic surface missions, and future crewed operations beyond low Earth orbit, all backed by a growing domestic workforce specialized in space disciplines.

Satellite Megaconstellations and Orbital Real Estate

China’s roadmap also reinforces its aggressive push into large satellite constellations.

Chinese entities have filed extensive applications with the International Telecommunication Union to reserve spectrum and orbital slots for future systems numbering in the hundreds of thousands over the coming decade. These filings secure scarce orbital resources while positioning China to compete directly with existing broadband constellations. Control over spectrum and orbital slots determines who can deploy at scale, who faces interference constraints, and who shapes future standards. China is acting early to lock in access, ensuring its operators retain strategic flexibility as orbital traffic intensifies.

For existing constellation operators, this signals tighter competition for spectrum coordination and growing geopolitical complexity in ITU processes.

Space Resources and the Groundwork for Off-Earth Utilization

While less detailed publicly, the five-year framework references space resource development as part of China’s medium-term objectives. This points toward future lunar utilization architectures, including in-situ resource extraction, surface logistics, and energy generation.

Resource development is being planned alongside launch systems, robotics, navigation, and power infrastructure, indicating a long-term vision for sustained off-Earth presence

rather than isolated exploration missions.

Over time, this approach supports permanent lunar operations and potential cis-lunar industrial activity.

What This Means

Taken together, China’s five-year plan represents a transition from space capability to space ecosystem design.

Tourism accelerates human-rated vehicles. Orbital computing drives constellation growth. Megaconstellations justify launch cadence. Deep-space programs advance propulsion and autonomy. Resource utilization supports permanent operations. Each pillar reinforces the others, forming a vertically integrated strategy for space commerce.

This contrasts with the Western model, where commercial development remains spread across agencies, regulators, and private operators. China is synchronizing state capital, industrial policy, education, and orbital planning into a unified framework.

For commercial actors, this reshapes competitive assumptions across tourism, satellite services, and space-based data markets.

For governments, it underscores the urgency of spectrum diplomacy, regulatory coherence, and international norms governing orbital infrastructure and space-based computing.

For everyone else, whether in the space industry or otherwise, it signals that by 2030 the world will be operating within an unprecedented, fully globalized space economy.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

War Series: How a U.S. Civil War Naval Doctrine Shapes Modern High Tech Supply Chain Arbitration

March 2, 2026

In 1863, during the height of the American Civil War, the British barque *Springbok* was intercepted by the USS *Sonoma* while sailing toward Nassau, a port in the neutral British Bahamas. The vessel's manifest listed a cargo of textiles, boots, and saltpeter, goods that were commercially standard and bound for a neutral jurisdiction. Under the strict letter of maritime law at the time, trade between neutral ports was protected. Yet, the U.S. Supreme Court eventually condemned the cargo. The court reasoned that while the ship would unload in Nassau, the cargo was meant to be transshipped to a blockade-runner and smuggled into the Confederate states.

This judgment established the doctrine of "Continuous Voyage" (or "Ultimate Destination"): the principle that the legality of a shipment is determined not by the initial port of discharge, but by the ultimate intent of the goods. The voyage was deemed "continuous" despite the stopover, and the neutral port provided no sanctuary if it was merely a waypoint for contraband.

Decades later, during World War I, the British Prize Court expanded this doctrine in the case of *The Kim* (1915). Authorities seized American cargoes of lard and wheat bound for Copenhagen, a neutral port, on the statistical inference

that the volume of goods vastly exceeded Danish consumption requirements. The precedent was set: the legal “voyage” ignores the physical itinerary and follows the goods to their final end-user.

Today, physical naval blockades have largely been replaced by regulatory architectures, export controls, sanctions, and entity lists. However, the ghost of the *Springbok* haunts the modern semiconductor and high-tech supply chain. The logic of “Continuous Voyage” has been digitized, shifting the burden of enforcement from naval captains to corporate compliance officers, creating a volatile new arena for private commercial disputes.

The Modern Pivot: From Ports to Proxies

In the modern high-tech economy, the “neutral port” is no longer a physical harbor like Nassau or Rotterdam. Instead, it is a Distributor or a Trading House located in a jurisdiction that is politically non-aligned or legally distinct from sanctioned territories. The “contraband” is no longer boots or salt, but dual-use integrated circuits, semiconductor manufacturing equipment, and encryption software.

The regulatory expectation today mirrors the 19th-century doctrine: authorities disregard the invoice address. If a supplier in Country A ships advanced processors to a distributor in Country B, and those processors are likely to be re-exported to a restricted entity in Country C, the trade is viewed as a direct violation by the supplier. The voyage is continuous.

The critical difference, however, lies in execution. In 1863, the state enforced the blockade. In the 2020s, the state has deputized the private sector. Manufacturers are required to look past their contractual counterparty and assess the “ultimate destination.” This deputization has sparked a wave of Business-to-Business (B2B) friction that is increasingly

ending in international arbitration.

The Private Sector Conflict

The core of the modern dispute is not between a government and a company, but between a Supplier (seeking compliance) and a Distributor (seeking performance).

Consider a common scenario: A Supplier of high-tech components enters a long-term framework agreement with a Distributor in a neutral third country. Mid-contract, geopolitical tensions rise, and export controls are tightened. The Supplier's internal compliance software flags the Distributor's jurisdiction as a high-risk transshipment hub. Fearing strict liability or loss of export privileges, the Supplier suspends shipments, citing "suspected diversion."

The Distributor, however, declares a Breach of Contract. They argue that they are a legitimate business, the goods are for local civilian use, and the Supplier is reacting to paranoia rather than law. The Distributor initiates arbitration, seeking damages for lost profits and reputational harm.

Here, the Supplier is trapped in a pincer movement. If they ship, they risk existential regulatory penalties from their home government. If they refuse to ship without concrete proof of diversion, they face millions in damages for breach of contract.

Legal Analysis in Arbitration: The Burden of Proof

When these disputes reach an arbitral tribunal, the central legal battleground is the burden of proof and the definition of "Force Majeure" or "Illegality."

The Distributor typically argues that a contract can only be voided by *actual* illegality. They assert that unless the government has specifically listed them as a sanctioned entity, the Supplier has no right to withhold performance.

From this perspective, the Supplier's refusal is a voluntary business decision to de-risk, not a legal necessity.

The Supplier, invoking the spirit of "Continuous Voyage," argues that the *risk* of diversion creates a constructive illegality. They assert that modern compliance standards require "Know Your Customer" (KYC) diligence that goes beyond government lists. If a Supplier ignores "Red Flags", such as a Distributor ordering volumes inconsistent with local demand (echoing the lard statistics of *The Kim*), they can be held liable.

This creates a complex question for arbitrators: **Is reasonable suspicion enough?**

If a tribunal demands "concrete evidence" that goods will be diverted, the Supplier will almost always lose. Proving a future negative, or proving the intent of a third party three steps down the supply chain, is nearly impossible without subpoena powers the private sector lacks. However, if the tribunal accepts "reasonable suspicion" as a valid ground for Force Majeure, it grants Suppliers immense power to unilaterally void contracts based on internal risk appetites, potentially destabilizing global trade reliability.

Furthermore, the role of the End-User Certificate (EUC) is under scrutiny. Historically, an EUC signed by the buyer was a shield, a document the Supplier could rely on to prove good faith. In the modern era of "Continuous Voyage," the EUC is increasingly viewed as a "rebuttable presumption." Tribunals are asking whether the Supplier *should have known* the EUC was merely a paper promise. Did the Supplier conduct due diligence, or did they willfully ignore the reality of the trade route?

Conclusion: The "Reasonableness" Standard

The revival of the "Continuous Voyage" doctrine in the form of digital supply chain controls suggests that the era of

simplified global trade is over. For legal practitioners and corporate officers, the takeaway is twofold.

First, standard “Force Majeure” and “Compliance with Laws” clauses are no longer sufficient. Contracts must now include specific “Sanctions and Export Control” clauses that explicitly grant the Supplier the right to suspend or terminate performance based on *reasonable internal assessment* of risk, not just upon a final government ruling.

Second, the outcome of future arbitrations will likely hinge on the concept of “abuse of right.” Tribunals will look for a balance: Did the Supplier act in good faith to comply with complex regulations, or did they use regulatory ambiguity as a convenient excuse to exit a commercially unfavorable contract?

Just as the *Springbok* case forced maritime law to look beyond the immediate horizon, modern high-tech trade requires companies to look beyond the immediate invoice. The voyage is continuous, and so is the liability.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/