War Series: The Cyber-Kinetic Blur — 27+ Data Center Strikes in Active Conflicts, the NotPetya Precedent, and "Acts of War" in Arbitration

October 19, 2026

In the architecture of global commerce, risk is fundamentally priced against historical precedent. For decades, that precedent dictated a clearly defined paradigm: warfare was kinetic, geographic, and overt. Standard *force majeure* provisions and property insurance "war exclusions" were meticulously calibrated for a world of naval blockades, physical destruction, and formal declarations of hostility. If a sovereign state committed an act of war, the evidentiary threshold was unmistakable, and the contractual remedies were clear. That framework is now structurally obsolete. As highlighted by a recent *NBC News* analysis documenting at least 27 direct attacks on data centers across active global conflicts, the civilian digital infrastructure that underpins the global economy is no longer merely collateral damage; it has become a primary military target. This escalation signals a definitive new front in modern warfare, where state-sponsored operations, whether kinetic strikes on centralized data nodes or the deployment of weaponized malware, routinely serve as the vanguard of geopolitical friction. This reality erases sovereign borders, transforms neutral corporate supply chains into active conflict zones, and exposes how systematically the broader market is mispricing the associated legal risk.

For multinational capital and the legal counsel tasked with

its preservation, the 2017 *NotPetya* cyberattack remains the definitive baseline. Generating an estimated $10 billion in total global economic damage according to U.S. White House assessments, the event exposed a critical vulnerability: commercial contracts drafted for twentieth-century physical hostilities are highly susceptible to twenty-first-century digital contagion.

The Second-Order Effects of Insurance Risk Transfer

NotPetya was initially deployed against Ukrainian tax software, but the malware rapidly broke containment, paralyzing the operations of non-combatant commercial entities globally. When pharmaceutical conglomerate Merck & Co. suffered severe operational downtime, it sought relief under its "all-risk" property insurance policies. Underwriters denied the claim, invoking standard "war exclusion" clauses on the grounds that *NotPetya,* widely attributed to Russian military intelligence, was an uninsurable act of war.

The resulting litigation, *Merck & Co., Inc. v. Ace American Insurance Co.* (N.J. Super. Ct. App. Div., 2023), culminated in a ruling that standard "hostile action" exclusions applied exclusively to traditional, kinetic warfare. Merck and its insurers ultimately reached a confidential settlement in early 2024, reportedly resolving the $1.4 billion claim. Similarly, food and beverage giant Mondelez International settled a high-profile $100 million claim with Zurich Insurance in late 2022 following a comparable dispute.

However, viewing these settlements as definitive corporate victories ignores the second-order effects on the market. Recognizing the existential threat to systemic capital, the London insurance market, the historical epicenter of global risk allocation, fundamentally re-engineered its exposure. Effective March 31, 2023, the Lloyd's Market Association (LMA) issued Bulletin Y5381, mandating that all standalone cyber policies explicitly exclude liability for state-backed cyberattacks that "significantly impair the ability of a state

to function” (standardized under the LMA5564 series of clauses).

With insurers successfully transferring the liability of digital warfare back onto corporate balance sheets, the legal battleground has permanently migrated. Disputes over supply chain failures, data center outages, and operational downtime have shifted from insurance subrogation into the realm of business-to-business breach-of-contract and *force majeure* arbitrations.

A Seamless Global Contagion, Localized Liability

The primary danger for the modern enterprise is that digital supply chains and data center networks are hyper-integrated, yet the legal mechanisms to defend them remain fiercely localized. A single piece of malicious code, or a kinetic strike on a regional data center, can ripple across the global economy, intersecting with fundamentally different statutory frameworks in real time. Instead of neatly separated jurisdictions, legal departments must now navigate a seamless global threat vector that cascades across regional legal doctrines.

Consider the lifecycle of a modern digital disruption. If a state actor breaches an EU-based logistics network, the commercial dispute instantly morphs into a regulatory crisis. Authorities evaluate the breach against the stringent strictures of the NIS2 Directive (Directive (EU) 2022/2555). It is insufficient to merely claim geopolitical *force majeure* to excuse non-performance; if a corporate victim failed to implement baseline cybersecurity risk-management measures, they face regulatory fines of up to €10 million or 2% of their global annual turnover. Domestically, European tribunals may reasonably conclude that this prior compliance negligence renders any contractual *force majeure* defense void, as the disruption could have been prevented or mitigated.

Tracing those supply arteries further east, the hardware powering this global system is manufactured by the highly

integrated tech conglomerates of Japan and South Korea. According to IBM's 2024 X-Force Threat Intelligence Index, the Asia-Pacific region remains one of the most heavily targeted geographic areas globally. When commercial entities are disrupted by regional Advanced Persistent Threats (APTs), they confront rigid domestic civil codes. Seeking relief under the strict unforeseeability requirements of the Japanese Civil Code or the South Korean Civil Act is legally complex. In these jurisdictions, state-sponsored cyber hostility is increasingly scrutinized not as an unforeseeable act of war, but as a quantifiable, baseline operational risk that should have been priced into the contract.

This commercial vulnerability is accelerating rapidly in the Middle East. As the Gulf Cooperation Council (GCC), a regional cybersecurity market projected to exceed $13 billion by 2027, executes some of the most digitally integrated infrastructure megaprojects in history, legacy energy grids are evolving into hyper-connected smart cities. If state-sponsored malware targets a regional desalination plant or paralyzes automated port logistics, developers and sovereign wealth funds face immediate contractual deadlock. They must litigate whether the disruption constitutes a valid "extraneous cause" (*cause étrangère*) under statutes such as Articles 273 and 287 of the UAE Civil Transactions Law, or a fundamental failure of the contractor to secure the digital perimeter.

When these high-stakes, cross-border disputes inevitably rupture, they frequently flow into premier neutral arbitration hubs like Singapore. Institutions such as the Singapore International Arbitration Centre (SIAC) are increasingly tasked with adjudicating massive supply chain defaults caused by digital sabotage. Concurrently, Singapore's Cybersecurity (Amendment) Bill 2024 has expanded regulatory oversight to cover entities of "special cybersecurity interest," demonstrating how intimately commercial arbitration is becoming entangled with national security statutes. The traditional boundaries between private commercial disputes and sovereign regulatory regimes have vanished.

The Evidentiary Abyss of Attribution

Whether seated in Singapore, London, or Dubai, arbitral tribunals handling these disputes face a singular, paralyzing hurdle: the legal standard of attribution.

In kinetic warfare, attributing a physical strike on a facility to a sovereign state relies on observable fact. Cyberspace operates through proxies, criminal syndicates, and false-flag code. If a data center provider or logistics firm defaults on a major GCC infrastructure contract and invokes an "act of war" clause following a cyber event, establishing definitive state sponsorship before a private commercial tribunal is an immense evidentiary burden.

The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* outlines strict thresholds for attributing cyber operations to a state, but private commercial tribunals lack the investigative authority of sovereign intelligence agencies. Arbitrators must distinguish between a state military operation and financially motivated cybercrime on a balance of probabilities. Parties often attempt to introduce unclassified intelligence from national cyber authorities to bridge this gap. However, under frameworks like the IBA Rules on the Taking of Evidence, relying on classified or highly redacted state intelligence within private commercial disputes introduces significant procedural complexities and questions of geopolitical bias.

Pragmatic Imperatives for Capital Protection

As the recent targeting of data centers illustrates, the intersection of military strategy and civilian data infrastructure is no longer a theoretical risk; it is an active operational reality. Relying on century-old boilerplate language for modern infrastructure and supply chain agreements presents a severe fiduciary vulnerability. In an environment where code deployed in one hemisphere can trigger a multi-billion-dollar default in another before the market opens, commercial structures must adapt.

For legal counsel and executives structuring multi-jurisdictional agreements, risk mitigation requires precise contractual mechanics:

- **Decouple Cyber from Kinetic Warfare:** Contracts should identify whether state-sponsored cyberattacks, physical strikes on data centers, and ransomware constitute a distinct *force majeure* event, rather than relying on legacy "war, hostilities, or acts of foreign enemies" clauses. The contractual language must be as specific as the threat vector.
- **Price the Collateral Damage:** Supply chain agreements should mathematically quantify liability and delay damages for instances where a party is not the primary target of a cyber-hostility but suffers operational paralysis due to global digital contagion.
- **Hardwire Attribution Mechanisms:** To prevent evidentiary stalemates in arbitration, contracts should establish a pre-agreed standard for attribution. For example, parties may stipulate that a formal, public declaration from a recognized national authority (such as the U.S. CISA, the UK NCSC, or the Cyber Security Agency of Singapore) serves as *prima facie* evidence of a state-backed attack for the purposes of the agreement.

Geopolitical conflicts are increasingly executed across the physical and digital assets of private enterprises. Until the mechanics of international commercial law fully adapt to the realities of asymmetric warfare, the imperative lies with the private sector to strictly define, price, and contractually ring-fence its digital liabilities. In the modern commercial theater, an ambiguous contract is a quantifiable liability.

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