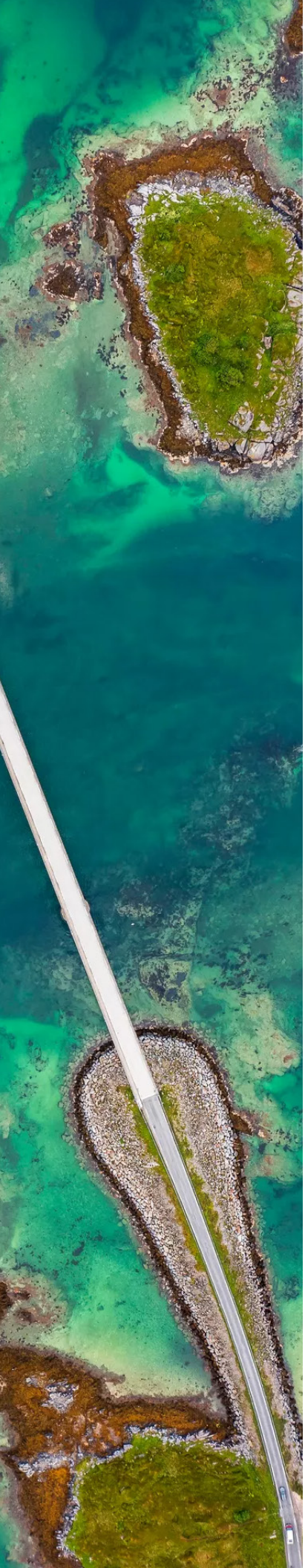
MOODY'S

Supporting Decision Dominance through Financial, Corporate, and Trade Intelligence

Table of Contents



1.0 Executive Summary: Supporting Decision Dominance

Government organizations rarely suffer from information scarcity. On the contrary, they are awash with data. This state often leads to decision friction: the difficulty of identifying what matters, connecting it across domains and institutions, and acting in time under conditions of uncertainty, legal constraint, and operational pressure. In a security environment shaped by reoccurring patterns and interconnected behaviors rather than isolated incidents, the quality of decisions is influenced by whether relevant information can be turned into actionable understanding before adversaries exploit delay, ambiguity, or fragmentation.

In security contexts, this challenge is well captured by the concept of **decision dominance:** the ability to observe, understand, decide, and act more effectively than adversaries, while preserving the freedom of action under pressure. But decision dominance is not simply a result of possessing more data. It can be understood as the operational outcome associated with combining relevant intelligence, analytical tradecraft, governance, and timely action in ways that improve judgment under constraint.

This paper argues that integrated financial, corporate, and trade intelligence can make a distinctive contribution to decision dominance by helping to illuminate the enabling networks behind multi-domain threats. Where operational data may show the tangible incident, these non-traditional forms of intelligence can help expose ownership, control, financing, logistics, dependencies, and intermediaries that may not be apparent from operational data alone. This matters because many of today's highest-priority threats are best understood not as isolated events, but as networked systems designed to exploit seams between domains, agencies, and jurisdictions.

Taking each security domain in turn—maritime, land, air, space, and cyber—this paper examines how the addition of this non-traditional intelligence can support more targeted, proportionate, and better-informed decision-making. It also addresses the practical requirements for doing so: cross-domain integration, analytical capability, governance, and carefully structured public-private collaboration.

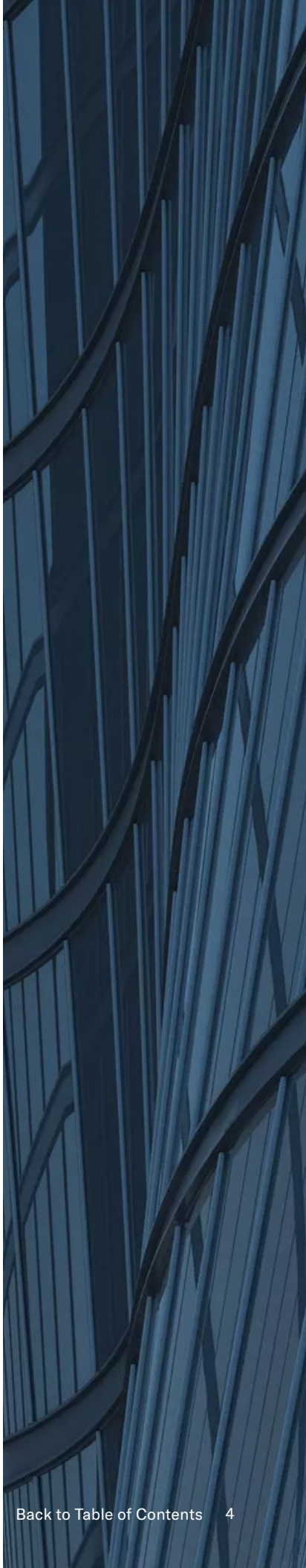
To ground this argument in real defense contexts, the paper includes brief illustrative examples drawn from recent operationally relevant work: (i) securing military logistics and supplier networks against hidden foreign ownership and malign influence, where rapid ownership resolution informed the assessment timeline; (ii) defense R&D supply chain analysis that extends from captured battlefield equipment into upstream enabling networks; and (iii) defense horizon scanning and risk profiling used to inform resilience and deterrence planning in a small-state context.

2.0 Introduction: The Decision-Making Challenge in a Multi-Domain Environment

The sophistication and scale of criminal and hostile activity has continued to increase in many contexts, exploiting globalized trade, financial systems, and digital infrastructure. Yet a central challenge for governments is not simply the presence of threat, nor even the availability of data. It is the persistent friction in decision-making process: the difficulty of recognizing which signals matter, understanding how they connect, and acting with sufficient speed and confidence to shape outcomes and maintain operational advantage.

While the operational domains—maritime, land, air, space, and cyber—are a useful framework for understanding where hostile activity occurs, the threats that matter most are rarely confined to a single domain. They are sustained by enabling networks of ownership, finance, logistics, procurement, infrastructure, and communication that cut across organizational and jurisdictional boundaries. In many cases, what is visible operationally is only the surface-level expression of a deep system of relationships that helps shape how resilient, covert, and scalable a threat can or has become.

This is where non-traditional intelligence such as integrated financial, corporate, and trade intelligence can have particular value. It does not seek to replace sovereign intelligence, operational collection, or expert human judgment nor pretend to altogether remove uncertainty. But it can make hidden or complex networks more legible, suggest additional avenues for investigations or analysis, support prioritization, and contribute to a more robust evidential basis for intervention. As ever, the objective is not perfect information. It is **decision dominance:** more informed decisions under constraint, made with greater speed, precision, and confidence to help preserve freedom of action.



3.0 Supporting Decision Dominance Across Operational Domains

3.1 Maritime Domain: Supporting Decisions in a High-Volume, High-Risk Environment

THREATS TO MARITIME DECISION-MAKING

Maritime environments are characterized by high volumes of legitimate activity alongside persistent risks such as trafficking, sanctions evasion, environmental crime, and infrastructure vulnerability. The scale and openness of maritime systems can allow adversaries to obscure illicit activity within normal trade patterns.

OPERATIONAL CONSTRAINTS

Maritime authorities often operate in a high-volume environment shaped by jurisdictional complexity, uneven enforcement capacity, and the exploitation of corporate structures, flags of convenience, and opaque ownership arrangements. Legitimate trade moves at scale, while illicit activity can be concealed within normal commercial patterns and across multiple jurisdictions. These conditions make it difficult to distinguish genuinely high-risk activity from routine movement and complicate the timely allocation of operational resources. The resultant friction can contribute to delays and missed opportunities.

High-volume trade environments shape threat detection and monitoring. For example, the **U.S. Bureau of Transportation Statistics's 2026 annual report** shares that the top 25 tonnage US ports handled over 1.87 billion short tons of cargo in 2023.

SUPPORTING DECISION DOMINANCE

Supporting decision dominance in the maritime domain is shaped in part by the ability to identify high-risk activity within large volumes of legitimate trade behavior. Vessel ownership and registration structures, flag changes, trade and shipping patterns, financial and corporate linkages, and route anomalies can help shed light on potential threat exposure that might otherwise remain obscured. When integrated effectively, this intelligence can support more targeted action based on a stronger network-level understanding of illicit activity, contributing to more efficient and well-supported enforcement decisions. This can help authorities operate with greater situational awareness and focus.

ILLUSTRATIVE USE CASE: SHADOW FLEET EXPOSURE THROUGH NETWORKED MARITIME ANALYSIS

The visible vessel is often only one part of the problem when it comes to understanding shadow fleet schemes. Recent sanctions and maritime advisories have described patterns that include frequent changes in flag or registration, vessel ownership routed through shell companies created to hold individual ships, opaque management arrangements across multiple jurisdictions, ship-to-ship transfers to obscure cargo origin, and manipulation or interruption of AIS transmissions. Around the world, sanctions authorities often must go beyond targeting vessels and tackle the management firms, service providers, and intermediaries involved in these operations.

For government and defense decision-makers, shadow fleet risk may be more fully understood by examining a ship's enabling network. A vessel may appear as if it is conducting routine commercial activity when viewed only through its immediate voyage data, yet look materially different once ownership history, management links, insurance questions, routing anomalies, ship-to-ship activity, and counterparty relationships are considered together. Analysts who incorporate this firmographic and trade intelligence can move from seeing isolated red flags to a more coherent picture of ownership, control, and potential exposure. This zooming out effect can support more targeted boarding, inspection, and sanctions enforcement as well as wider disruption activity.

3.2 Land and Border Domain: Prioritizing Decisions at Scale

THREATS TO BORDER DECISION-MAKING

Land and border environments account for some of the most difficult trade-offs in government decision-making. Essential to national prosperity, lawful mobility, and the functioning of supply chains they are persistent targets for trafficking, illicit trade, sanctions circumvention, organized immigration crime, and the cross-border movement of goods, funds, and people linked to wider criminal networks. For many government agencies, the challenge is not recognizing that risk exists; it is distinguishing the relatively small proportion of high-risk activity from the much larger volume of legitimate movement that must continue with minimal disruption.

Legal purchases paired with hand-offs to smugglers aids cross-border weapons trafficking: a **U.S. Government Accountability Office report** notes that the Mexican government has estimated that 200,000 firearms are smuggled from the United States into Mexico each year.

OPERATIONAL CONSTRAINTS

Border authorities must make decisions at scale under time pressure. Large volumes of passengers, freight, parcels, and conveyances pass through border checkpoints every day, while relevant information may remain fragmented across agency boundaries between customs, immigration, law enforcement, financial intelligence, and partner agencies. Legal thresholds for inspection, detention, or seizure must be met in a consistent and proportionate way, even as adversaries adapt quickly by changing routes, documentation, intermediaries, and methods of concealment. In practice, this means that border security is shaped in part by the ability to identify indicators that justify timely intervention and the quality of prioritization.

SUPPORTING DECISION DOMINANCE

Supporting decision dominance at the border largely depends on information that helps agencies move beyond surface-level declarations to a better understanding of underlying networks and exposure.
Customs records, trade documentation, supply-chain data, corporate ownership structures, and beneficial ownership information can help reveal anomalous routes, unusual trading relationships, mismatches between counterparties and commodities, and commercial patterns that do not align with expected behavior. These non-traditional forms of intelligence are particularly valuable where hostile or criminal actors make use of intermediaries, shell entities, freight forwarders, or layered commercial relationships to disguise the movement of illicit goods and the financing behind them.

When integrated effectively, this information supports more targeted border inspections with more defensible intervention decisions, and thus can contribute to better allocation of scarce operational resources. It allows agencies to focus attention where the combination of route, actor, commodity, ownership, and financial context indicates elevated risk, while reducing unnecessary friction for legitimate trade and travel. In this sense, information advantage at the border is not simply about identifying more risk; it is about enabling governments to act with greater precision, consistency, and confidence in an environment where speed and proportionality matter.

ILLUSTRATIVE CASE STUDY: PREVENTING CONTRACTS WITH THE ADVERSARY

Comparable challenges exist in military logistics: large volumes of third party suppliers, global operations crossing multiple jurisdictions, and persistent exposure to hidden foreign influence through layered corporate structures. In one U.S. defense land transportation context, defense analysts described the operational burden of stitching together data from disparate sources to assess who ultimately owned and influenced their supplier.

During a proof-of-concept exercise, Moody's ownership intelligence was used to help identify the global ultimate owner of an entity presented in the session, revealing a linkage to a state-owned enterprise. This type of analytic connection had previously taken the defense logistics command extended manual research to establish.

The value, in this context, was not additional data in isolation, but the ability to more efficiently connect ownership and corporate structure to vendor risk. Moody's structured and analyzed data supported more timely and better supported supplier decision-making, and helped inform assessments of exposure to potential malign influence within the defense logistics base.

3.3 Air Domain: Accelerating Time-Critical Decisions

THREATS TO AVIATION DECISION-MAKING

Aviation presents a distinct decision-making challenge because incidents can develop quickly, consequences can be severe, and windows for potential intervention are often narrow. Threats include the movement of illicit drugs and pre-cursor chemicals, sanctions evasion through aviation supply chain networks, misuse of charter or lightly regulated operators, and the growing use of drones to disrupt critical sites, surveillance activities, or transport infrastructure. Although the total volume of air movements may be lower than in maritime or land environments, the speed, reach, and potential strategic sensitivity of the air domain make accurate prioritization especially important.

OPERATIONAL CONSTRAINTS

Authorities operating in this domain must make time-critical judgments using information that may be distributed across passenger records, cargo manifests, operator histories, ownership data, financial information, and regulatory filings. International coordination is frequently required, but similar to the maritime and land domain, legal guidelines, reporting standards, and enforcement capacities differ across jurisdictions. At the same time, legitimate aviation infrastructure serves both civilian and strategic defense purposes, which can complicate decisions about escalation, inspection, interdiction, or follow-on investigation. The operational challenge, therefore, is not simply to detect anomalies, but to assess which anomalies may warrant further action and what form that action should take.

> Drones have changed the face of modern warfare, with large numbers reportedly manufactured and deployed in the Ukraine-Russia war. Operational awareness of adversary supply chains plays an important role in supporting decision dominance.

SUPPORTING DECISION DOMINANCE

Supporting decision dominance in the air domain is supported by the ability to rapidly connect operational and commercial signals. Flight manifests, cargo declarations, ownership and control data, compliance histories, financial linkages, and information on counterparties or logistics relationships can help identify flights, operators, or consignments that merit closer scrutiny. This is particularly important where illicit activity is embedded within legitimate traffic and where risk may only become visible when data is connected across multiple sources rather than viewed in isolation.

Using well-integrated intelligence can support earlier detection of unusual patterns, more proportionate intervention under uncertainty, and better sequencing of operational responses. It can help authorities distinguish between low-confidence anomalies and higher-risk combinations of behavior, ownership, route, and financial context. For decision-makers, the value lies not in eliminating uncertainty altogether, but in reducing ambiguity enough to act at speed when necessary and to justify that action afterwards.

ILLUSTRATIVE CASE STUDY: FROM CAPTURED DRONE SYSTEMS TO SUPPLY CHAIN INTELLIGENCE

The air domain increasingly includes threats enabled by rapidly proliferating systems such as drones. In a U.S. defense research and capability development setting, a team supporting warfighters recovered fallen drones on the battlefield, transferred them for technical analysis, and then examined them to identify the origin of component parts. This information supported further analysis of upstream supply chains and the companies enabling adversary aerospace capabilities.

This shifts investigative questions from “what is the system?” to “how is it enabled?” This is a critical distinction when the objective is to disrupt or mitigate capability upstream rather than respond only at the point of use. In this case, the program’s focus included developing the capability to analyze, visualize, and secure supply chains in support of U.S. defense planning and capability development.

For decision-makers, threat mitigation may increasingly be informed by efforts to identify the enabling network—suppliers, intermediaries, and ownership structures—behind systems that create operational risk.

3.4 Space Domain: Managing Dependency and Resilience

THREATS TO SPACE DECISION-MAKING

Space is a critical domain for enabling activity across government, defense, the global economy, and many other domains. Communications, positioning, navigation, timing, remote sensing, weather services, and intelligence collection all depend, to varying degrees, on space-based infrastructure. As a result, threats in this domain are significant not only because of what happens on orbit, but because disruption can cascade into military operations, critical national infrastructure, financial systems, transport networks, and emergency response. The decision-making challenge is therefore less about viewing space as a separate specialist issue and more about understanding it as a strategic dependency whose degradation can affect multiple domains at once.

OPERATIONAL CONSTRAINTS

Operationally, space decisions are shaped by limited sovereign control, long development timelines, and heavy dependence on commercial providers, allied capabilities, and globally distributed supply chains. Governments may rely on infrastructure they do not fully own, manufacture, or operate, while the components and services that support space systems often involve complex chains of finance, subcontracting, and international dependency. This creates a difficult environment for prioritization: vulnerabilities may emerge not only from hostile action, but from concentration risk, supplier fragility, multi-jurisdictional regulatory exposure, or the failure of a critical commercial partner. Decision-makers therefore benefit from visibility not just into technical capability, but into the resilience and trustworthiness of the broader ecosystem on which that capability depends.

A 2025 **U.S. Government Accountability Office report** on the defense industrial base estimates that over 200,000 suppliers help produce advanced weapon systems and noncombat goods, but has limited visibility into the origin of these goods, their component parts, and raw materials.

SUPPORTING DECISION DOMINANCE

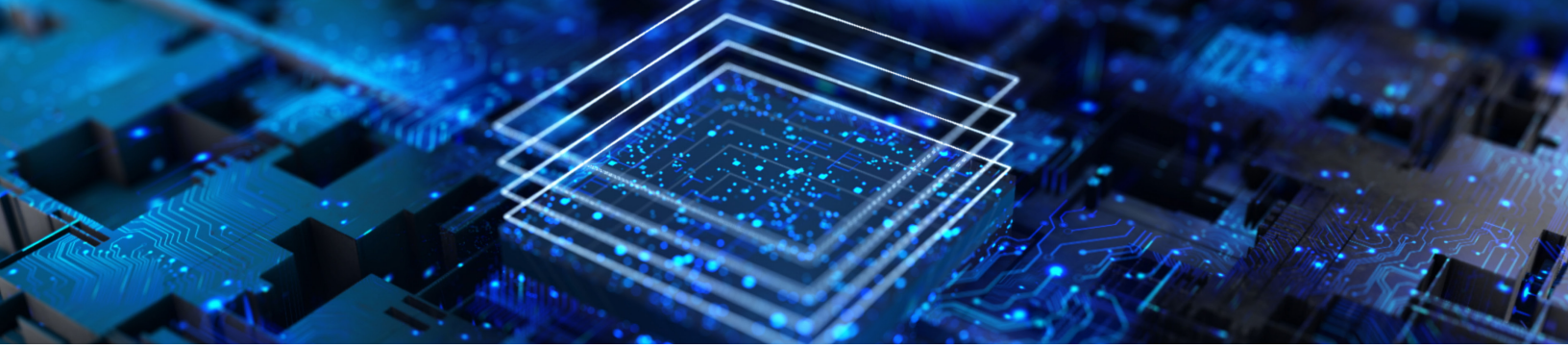
Supporting decision dominance in the space domain often demands an understanding of dependencies that are often less visible in purely technical assessments. Ownership structures of space operators, the composition of upstream and downstream supply chains, investment relationships, financial health, sanctions exposure, and reliance on single points of failure can all affect the resilience of a capability. These factors matter because they shape whether a government may be able to sustain access, trust the integrity of a service, or absorb disruption without disproportionate operational impact.

When integrated effectively, this information helps decision-makers identify concentration risk, prioritize resilience measures, and make better-informed procurement, partnership, and contingency planning decisions. It supports a more complete view of which capabilities are mission-critical, which dependencies require diversification, and where commercial or international reliance may create strategic vulnerability. In the space domain, decision advantage is closely tied to resilience: the ability to understand dependency early enough to help preserve freedom of action when systems are contested, degraded, or denied.

ILLUSTRATIVE CASE STUDY: HORIZON SCANNING FOR RESILIENCE AND DETERRENCE PLANNING

A different but strategically important defense case study is provided by a ministry of defense in the Asia-Pacific region. In the engagement, the ministry sought to scan the horizon for potential early warning signals and awareness of what might be coming, alongside developing risk profiles of ultimate beneficial owners and strengthening the information base supporting defense decision-making.

For the space domain, decision-makers may find dependency is a core issue: space capabilities and the services they enable depend on extended commercial and supply ecosystems. Horizon scanning and risk profiling can help decision-makers identify concentration risk and exposure earlier—supporting procurement resilience, diversification decisions, and contingency planning rather than reactive response after disruption.



3.5 Cyber Domain: Linking Digital Activity to Real-World Impact

THREATS TO CYBER DECISION-MAKING

Cyber threats create a particularly demanding decision environment because technical activity, criminal enterprise, and state-linked behavior often overlap. Ransomware, intrusion activity, data theft, critical infrastructure targeting, sanctions evasion, online fraud, and influence operations may appear distinct at first sight, yet they frequently rely on shared enabling networks of finance, infrastructure, intermediaries, and service providers. Cyber activity can also act as a force multiplier for threats in other domains, supporting disruption, concealment, coercion, and illicit movement through digital means.

OPERATIONAL CONSTRAINTS

Operationally, cyber decisions are complicated by attribution difficulty, compressed timelines, and fragmented legal and organizational responsibilities. Relevant evidence may sit across technical telemetry, payment flows, corporate registries, hosting infrastructure, open-source reporting, and partner intelligence, often spread across several jurisdictions and largely dependent on privately owned infrastructure. Agencies often must therefore make consequential risk management decisions related to disruption, escalation, notification, and coordination before a full picture is available. In such circumstances, speed matters, but so do evidential standards, proportionality, and an understanding of the broader economic and strategic context in which technical activity is occurring.

According to **Verizon's Data Breach Investigation Report (DBIR)**, an increased reliance on third-party software and services has increased organizations' attack surface, resulting in a 60% increase in breaches with third-party involvement in 2025.

SUPPORTING DECISION DOMINANCE

Supporting decision dominance in cyberspace largely depends on the ability to connect technical indicators with financial, corporate, and behavioral context. Cyber threat intelligence may indicate infrastructure, malware families, intrusion methods, or targeting patterns, but those signals can become more actionable when linked to payment flows, ownership structures, sanctions exposure, adverse media, and other forms of investigative intelligence. This broader context can help authorities identify not only who may be responsible, but also which intermediaries, commercial entities, and financial channels may be associated with the malicious activity.

This matters because effective cyber response is rarely a purely technical exercise. Disrupting malicious cyber threats often depends on coordinated action across law enforcement, intelligence, regulators, financial institutions, infrastructure operators, and international partners. Integrated intelligence helps decision-makers consider where intervention may be more impactful, whether by informing actions related to disrupting financial flows, exposing enabling networks, prioritizing defensive measures, or coordinating cross-agency response. In the complex and ever-evolving cyber and electromagnetic domain, integrated intelligence plays an important role in supporting timely, proportionate, and well-contextualized decision-making under uncertainty.

4.0 Cross-Domain Integration: Enabling Decision Advantage

Operational activity across maritime, land, air, space, and cyber environments is increasingly interconnected. A sanctions evasion network may rely on shipping movements in one domain, shell companies and trade intermediaries in another, digital communications in a third, and financial transfers running across several jurisdictions simultaneously. Risks that appear domain-specific are therefore often more fully understood when viewed as part of a wider system.

Consider a sanctions evasion network moving dual-use goods. The operational signature may first appear as a shipment taking a circuitous route, an extra intermediary, an unusual payment pattern, or suspicious digital communications. But the network itself may span shell companies in multiple jurisdictions, vessels or aircraft operating through permissive or corrupt regulatory environments, logistics brokers obscuring counterparties, and financial channels designed to distance the end user from the ultimate beneficial owner. No single domain view is likely to capture the broader picture. The decision advantage often lies in connecting fragmented data quickly enough to identify the enabling network behind the visible transaction.

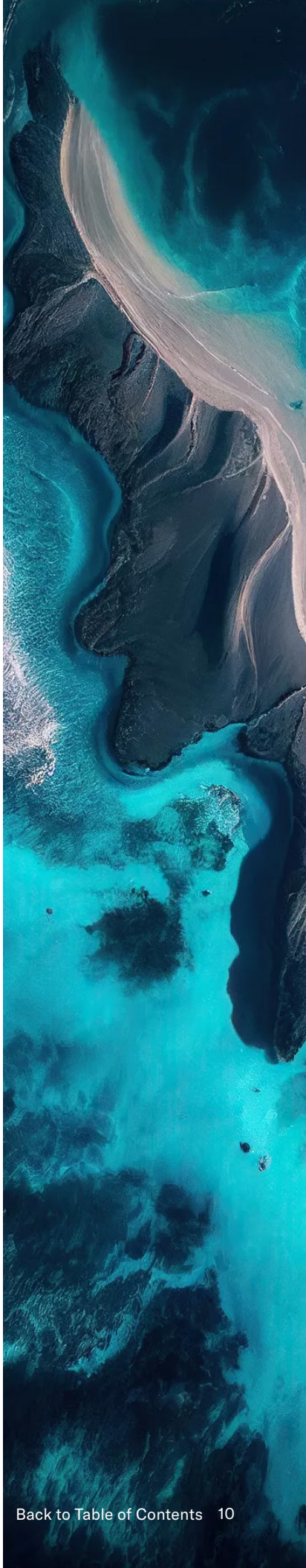
This is why cross-domain integration matters. National security and defense decision-makers often do not need more raw data; they need a coherent picture that connects entities, transactions, movements, and behaviors across boundaries. When intelligence remains siloed by function or domain, analysts must work harder to join the dots and authorities risk missing the relationships that help distinguish a routine event from a strategic threat. Integrated data environments can help reduce that risk by allowing analysts to move more rapidly from time-consuming data gathering and fragmented indicators to a more robust and well-supported assessment of intent, capability, and impact.

Financial, corporate, and trade intelligence can provide the connective tissue across domains, helping to clarify who ultimately owns or controls an asset, how a network is financed, which counterparties and routes create exposure, and where patterns of behavior deviate from the norm. Used effectively, this intelligence can support more targeted investigations, stronger prioritization of scarce resources, and closer coordination between agencies responsible for security, enforcement, intelligence, and policy.

DEFENSE SUPPLY CHAIN MONITORING: A CROSS-DOMAIN DISCIPLINE

This cross-domain reality is particularly visible in defense supply chains, which are exposed simultaneously to geopolitical shocks, cyber threats, non-transparent vendor ecosystems, and financial or reputational risk. Defense supply chains are described internally as nonlinear, expansive, mutually connected systems that therefore benefit from an architecture capable of continuous enhanced due diligence through assessment, reporting, and mitigation of threats and vulnerabilities across the material lifecycle.

One practical way to approach such a framework is through four pillars: (1) classification of supply chain security through an effective risk management framework; (2) data integrity and access, including protection of systems and remediation of cyber risks; (3) valid and reputable partners and vendors, including visibility of vendor and sub vendor relationships to mitigate fraud and counterfeit exposure; and (4) resilience of systems, processes, infrastructure, and people supported by actionable intelligence that strengthens continuity of operation.



5.0 Role of Data and Partnerships: Enabling Better Decisions

DATA AS AN OPERATIONAL ENABLER

Data contributes effectively to security and defense missions when it is aligned to operational decisions. For government users, that means having access to information that is relevant, traceable, structured, and capable of being integrated with existing workflows. High-volume data without context can slow decisions or obscure material risk. By contrast, well-curated financial, firmographic, trade, and adverse media information can help analysts identify meaningful anomalies, test hypotheses, and build a more defensible basis for action. At the same time,
no commercial or external dataset is complete, uniformly reliable, or sufficient on its own. Such data should therefore be treated as a complement to sovereign capability, not a substitute for it.

This is especially important in environments where intervention carries legal, diplomatic, or operational consequences. Decision support should therefore do more than surface alerts. It should help users understand provenance, ownership, exposure, and network relationships in a way that stands up to scrutiny and supports proportionate action. In this sense, high-quality data is not simply an input to analysis; it is part of the foundation for accountability, coordination, and operational confidence.

PUBLIC-PRIVATE COLLABORATION

A significant proportion of the data relevant to modern threat analysis sits outside government, held by commercial providers, financial institutions, logistics operators, insurers, and technology firms. As a result, public-private collaboration is often a practical requirement in many mission areas. But collaboration also raises legitimate questions about mutual assurance, governance, provenance, legal authority, and the secure handling of sensitive workflows. The same process of vetting upstream suppliers in defense logistics is relevant for evaluating the technology providers that provide insights into defense logistics investigations: an agency's choice of industry partner should be guided by the need to protect sovereignty, preserve trust, and improve decision quality.

Effective partnerships depend on clear alignment to mission needs. Data providers should be able to demonstrate source provenance, auditability, and an understanding of how their information will be used in operational settings. They should also be capable of supporting secure integration, enabling government users to enrich internal holdings without undermining control of sensitive environments. Where these conditions are met, partnerships can help agencies support investigative and analytical work, refine prioritization, and broaden visibility into networks that may otherwise remain fragmented.

6.0 Analytical Capability: From Data to Decisions

Even the richest data environment will have limited value without the analytical capability to interpret it. A central challenge for many organizations is not the absence of tools, but the difficulty of converting multiple data streams into decision-ready insight. That requires a combination of technology, tradecraft, and institutional processes that allow analysts to connect disparate indicators, assess competing explanations, and present findings in a form that security and defense decision-makers can consider and act on with confidence.

In practice, this means investing in capabilities that support entity resolution, network analysis, anomaly detection, and the integration of structured and unstructured data sources where appropriate. It also means supporting analysts' abilities to work across traditional domain boundaries, drawing together commercial, financial, operational, and investigative information rather than treating each as a separate discipline. For senior decision-makers, the value lies in receiving clearer options, stronger evidential grounding, and a better understanding of uncertainty and risk.

Analytical capability should therefore be designed to support, not replace, human judgment. In government and defense settings, decisions often carry strategic, legal, and ethical implications that can't be delegated to automated processes alone. The strongest analytical environments tend to be those that improve transparency, enable challenge, and help decision-makers understand not only what the data suggests, but also what it does not yet explain.

7.0 Recommendations: Building Decision Dominance

First, governments should consider **organizing data and analysis around priority operational decisions rather than around datasets or systems.** A more effective starting point may be to identify the decisions that matter most—such as inspection, interdiction, disruption, escalation, or resilience planning—and then determine what information is required to improve those decisions.

Second, agencies should consider **integrating ownership, finance, logistics, and supply-chain intelligence into existing operational workflows.** Many high-priority threats are sustained by hidden enabling networks. Improving visibility into those networks can strengthen prioritization, targeting, and case-building across domains.

Third, governments should consider **investing in the governance conditions that make integrated intelligence usable:** data provenance, auditability, legal clarity, secure integration, and appropriate challenge mechanisms. In many environments, the limiting factor is not technical possibility but the confidence that data can be used lawfully, proportionately, and defensibly.

Fourth, authorities should continue to **adopt risk-based approaches to resource allocation.** Universal coverage is unrealistic across modern operational environments. Integrated intelligence is often most valuable when it helps limited personnel and capabilities focus on the actors, routes, assets, and networks that present the greatest operational or strategic risk.

Fifth, **investment in data should be matched by investment in analytical tradecraft and institutional capability.** Tools and datasets create the greatest value when analysts can test hypotheses, connect indicators across domains, challenge assumptions, and present uncertainty clearly enough for decision-makers to act with confidence.

Sixth, **public-private collaboration should be treated as a strategic enabler, but not without qualifications.** The most effective partnerships are those built on transparency, secure integration, clear mission alignment, and a realistic understanding of what external data can and cannot provide. Commercial insight is most powerful when it complements sovereign capability and operational expertise.

Finally, **resilience should remain a key indicator of whether decision dominance has been achieved.** The objective is not merely to act quickly in favorable conditions, but to help preserve freedom of action when information is incomplete, systems are disrupted, and adversaries are deliberately generating ambiguity. Investment in integration, governance, and analytical discipline is therefore also an investment in resilience under pressure.

8.0 Conclusion: Decision Dominance as a National Imperative

For governments, a key challenge is not simply to collect more information, but to reduce decision friction. In an environment defined by complexity, speed, and cross-domain interdependence, advantage increasingly depends on timely understanding of situations, improved insight into the enabling networks behind visible events, and the ability to act with greater confidence than those seeking to exploit uncertainty.

Integrated financial, corporate, and trade intelligence can make a distinctive contribution to that objective by helping to clarify ownership, control, financing, logistics, and dependency across domains. It does not remove all uncertainty, and it can't replace sovereign intelligence or operational expertise. But it can help make complex or hidden networks more legible, support prioritization, and inform decisions that are more targeted, proportionate, and well-supported.

The organizations best positioned to succeed are likely to be those that connect data to mission needs, integrate insight across institutional and operational boundaries, and build the governance and analytical discipline that support the ability to act under pressure. The objective is not perfect foresight. It is sustained decision dominance: the ability to make sound decisions at the right time, with sufficient clarity to support the protection of national interests and public safety.

MOODY'S

Moody's Data and Analytics Solutions for Governments

Learn more about **Moody's corporate, financial, and trade intelligence for government missions worldwide.** If you'd like a tailored demonstration of how our data and insights can be used for your national security or defense use case, please **reach out.**