Adversarial Targeting of Commercial Logistics Networks: An Attribution Framework

Michael A. Torres

PLIANT Institute, Palo Alto, CA

Journal of Intelligence and National Security Studies, Vol. 12, No. 2 (August 2024), pp. 78–112

Abstract

Nation-state actors have increasingly targeted commercial logistics networks as instruments of geopolitical competition, economic coercion, and intelligence collection. Despite the operational significance of this threat, the analytical frameworks available to researchers and practitioners for identifying, characterizing, and attributing adversarial targeting of logistics infrastructure remain underdeveloped relative to frameworks applied to more traditional targets of state-sponsored activity. This paper develops a structured attribution framework for adversarial logistics targeting, drawing on open-source intelligence methodology, declassified government assessments, and a retrospective analysis of 94 documented targeting incidents across six threat actor categories between 2015 and 2023. The framework integrates technical indicators, behavioral patterns, targeting logic, and geopolitical context into a five-dimension attribution confidence assessment that is operationally deployable by both government analysts and private sector security teams. Implications for supply chain security policy and intelligence sharing between public and private sector actors are discussed.

Keywords: attribution, nation-state targeting, logistics networks, OSINT, supply chain security, adversarial behavior

---

1. Introduction

The weaponization of commercial logistics infrastructure by nation-state actors represents one of the most consequential and least analyzed dimensions of contemporary geopolitical competition. Unlike cyber intrusions targeting government systems or military networks — which have attracted substantial analytical attention and generated well-developed attribution methodologies — adversarial activity targeting commercial logistics occupies an analytically ambiguous space where the tools of intelligence analysis, supply chain security, and geopolitical risk assessment converge without adequate institutional infrastructure to support rigorous attribution work.

This ambiguity is not incidental. It reflects the structural characteristics of logistics targeting as a form of state-sponsored activity: the commercial environment in which incidents occur provides natural deniability; the heterogeneous population of potential disruption causes — equipment failures, labor actions, weather events, criminal activity — creates attribution noise; and the distributed nature of global logistics networks means that no single government or private actor has visibility across the full operational environment. State actors have exploited these characteristics systematically, conducting targeting operations that impose meaningful costs on adversaries while maintaining comfortable distance from formal attribution.

The analytical gap this creates has direct operational consequences. Private logistics operators experiencing anomalous disruptions cannot distinguish between routine operational failures and deliberate adversarial activity

without analytical frameworks they typically lack. Government agencies with relevant intelligence struggle to share actionable attribution assessments with private sector actors through channels adequate to the operational tempo of logistics disruption. And the research community, lacking a shared methodological foundation for logistics targeting attribution, has produced findings that are difficult to accumulate or generalize.

This paper addresses the analytical gap by developing a structured attribution framework specifically calibrated to the characteristics of adversarial logistics targeting. The framework draws on the author's prior experience in government intelligence analysis and on the body of open-source and declassified materials that has accumulated around documented logistics targeting incidents over the past decade. It is designed to be operationally useful — applicable by analysts with varying levels of classified access — while maintaining the methodological rigor that attribution assessments require.

2. The Landscape of Adversarial Logistics Targeting

Before developing the attribution framework, it is useful to characterize the landscape of adversarial logistics targeting that the framework is designed to address. Four primary targeting vectors have emerged from the incident record and from declassified government assessments of state-sponsored logistics activity.

2.1 Procurement Manipulation

Procurement manipulation involves the insertion of state-linked actors into critical supply chains through bid manipulation, regulatory capture, shell company structures, and the exploitation of procurement processes that lack adequate beneficial ownership transparency. This vector enables persistent access to logistics infrastructure, intelligence collection on commercial and government supply chain dependencies, and the capacity to disrupt or degrade logistics performance at operationally significant moments. Procurement manipulation is the most difficult targeting vector to detect and attribute because it operates through ostensibly legitimate commercial channels and leaves limited technical artifacts.

2.2 Logistics Data Falsification

Data falsification encompasses the manipulation of manifests, bills of lading, customs declarations, and cargo tracking systems to conceal sanctioned goods, enable intelligence collection on trade flows, or disrupt customs enforcement mechanisms. This vector has been documented extensively in the context of sanctions evasion but is less well understood as a deliberate intelligence operation. Advanced data falsification operations exhibit characteristics — timing, target selection, operational security — that are inconsistent with purely commercial motivations and suggest state direction or facilitation.

2.3 Cyber-Physical Attack

Cyber-physical attacks targeting logistics infrastructure range from ransomware operations against terminal operating systems to more sophisticated intrusions designed to produce physical disruption through digital means. This vector has received the most analytical attention of the four, partly because it leaves technical artifacts that support attribution analysis and partly because it aligns with existing cyber threat intelligence frameworks. However, the logistics-specific dimensions of cyber-physical targeting — target selection logic, operational timing, desired disruption outcomes — are less well characterized than the technical intrusion methods themselves.

2.4 Human Intelligence Cultivation

Human intelligence cultivation involves the long-term development of logistics sector personnel as sources of operational intelligence, insider access, or facilitation of other targeting vectors. This is the least visible and

arguably most consequential targeting vector, as cultivated sources can provide persistent access to operationally sensitive information across multiple facility and organizational boundaries. Cultivation operations are rarely detected in real time and are typically reconstructed retrospectively from other evidence of targeting activity.

3. Attribution Framework Development

The attribution framework developed in this paper rests on five analytical dimensions, each of which captures a distinct category of evidence relevant to determining whether a logistics disruption event reflects deliberate adversarial activity and, if so, which actor category is most plausibly responsible.

3.1 Technical Indicators

Technical indicators are artifacts of the targeting operation that can be observed and analyzed independent of the broader operational context. For cyber-physical attacks, technical indicators include malware signatures, intrusion TTPs, infrastructure characteristics, and forensic artifacts recoverable from affected systems. For data falsification operations, technical indicators include document metadata, formatting anomalies, and system access logs. For procurement manipulation, technical indicators are more limited but may include corporate registry anomalies, beneficial ownership discrepancies, and financial flow irregularities accessible through open-source research.

Technical indicators support attribution most reliably when they can be linked to previously characterized threat actor infrastructure or operational patterns. Attribution based solely on technical indicators should be treated as hypothesis-generating rather than conclusive, as technical indicators can be spoofed and are subject to false flag operations by sophisticated actors.

3.2 Behavioral Patterns

Behavioral patterns refer to the operational characteristics of the targeting activity that persist across incidents and are difficult to modify without significantly changing operational effectiveness. In the logistics targeting context, relevant behavioral patterns include the timing and tempo of operations, the selection criteria applied to targets within a broader opportunity set, the level of operational security maintained, and the apparent tolerance for attribution risk. Behavioral patterns are more robust attribution indicators than technical artifacts because they reflect organizational culture and resource constraints that are difficult to fake consistently.

3.3 Targeting Logic

Targeting logic analysis asks whether the observed disruption pattern makes strategic sense from the perspective of each candidate threat actor. An actor seeking economic coercion leverage will target nodes with high throughput concentration and limited bypass alternatives; an actor seeking intelligence collection will target nodes with maximum visibility into trade flows of strategic interest; an actor seeking to demonstrate capability will target high-profile nodes with maximum media salience. Targeting logic analysis requires a well-developed model of each candidate actor's strategic objectives and operational constraints, which is the most demanding analytical input to the framework.

3.4 Geopolitical Context

Geopolitical context situates the observed targeting activity within the broader pattern of state behavior during the relevant period. Escalation in bilateral tensions, upcoming diplomatic events, domestic political pressures, and parallel operations in other domains all provide contextual signal that can sharpen or constrain attribution assessments. Geopolitical context is particularly valuable for distinguishing between candidate actors with similar technical signatures or behavioral patterns, as their geopolitical motivations for targeting a specific node at a specific time may differ substantially.

3.5 Corroborating Intelligence

Corroborating intelligence encompasses information from sources external to the incident itself that is relevant to attribution — including partner-shared government intelligence, OSINT from adjacent domains, and information from other affected parties. Corroborating intelligence can substantially strengthen attribution confidence when it converges with the technical, behavioral, and contextual indicators from the incident analysis. The challenge of incorporating corroborating intelligence in a structured framework is that its quality and credibility vary substantially across sources, requiring explicit confidence weighting rather than simple aggregation.

4. Attribution Confidence Assessment

The five-dimension framework supports a structured confidence assessment that communicates both the direction of attribution and the evidentiary basis for it. Attribution confidence is assessed on a three-level scale: High confidence requires convergent evidence across at least three dimensions with no contradicting indicators; Medium confidence requires evidence across at least two dimensions with no strong contradicting indicators; Low confidence reflects single-dimension evidence or conflicting indicators across dimensions.

Across the 94-incident retrospective dataset, the framework produces High-confidence attribution in 31% of cases, Medium-confidence in 38%, and Low-confidence or indeterminate in the remaining 31%. The High and Medium confidence cases are concentrated among incidents involving cyber-physical attacks, where technical indicators are richest, and among incidents where corroborating intelligence was available through PLIANT's partner network. Low-confidence cases are concentrated among procurement manipulation incidents, where technical indicators are sparse and behavioral pattern evidence is thin.

5. Application to Threat Actor Categories

The framework has been applied to incidents attributable to six threat actor categories in the retrospective dataset: People's Republic of China state-linked actors, Russian Federation state-linked actors, Iranian state-linked actors, North Korean state-linked actors, non-state criminal actors with possible state facilitation, and indeterminate actors. Each category exhibits distinct signatures across the five attribution dimensions that, when aggregated across multiple incidents, support reliable differentiation.

PRC state-linked actors exhibit the highest operational sophistication and the most consistent targeting logic across the dataset, with a strong preference for procurement manipulation and human intelligence cultivation over technically attributable cyber-physical attacks. Russian state-linked actors show higher tolerance for attribution risk, with a larger share of cyber-physical attacks carrying technical signatures linkable to known threat actor infrastructure. Iranian and North Korean state-linked actors exhibit more opportunistic targeting patterns with less consistent strategic logic, suggesting operational constraints that shape target selection.

6. Policy Implications

The attribution framework developed here has direct implications for how government agencies and private sector actors approach logistics targeting incidents. Three implications are worth emphasizing. First, attribution is a continuous analytical process rather than a binary determination — the framework supports incremental confidence updates as new evidence becomes available, which is more operationally useful than waiting for certainty before acting. Second, the private sector actors most exposed to logistics targeting rarely have access to the full evidence set that high-confidence attribution requires — closing this gap requires more robust intelligence sharing frameworks than currently exist. Third, the concentration of high-confidence attribution capacity in cyber-physical incidents creates incentives for sophisticated actors to operate through less technically attributable

vectors, which the current analytical and policy infrastructure is poorly positioned to address.

7. Conclusion

Adversarial targeting of commercial logistics networks is a consequential and analytically underserved problem. The framework developed in this paper provides a structured approach to attribution that is calibrated to the specific characteristics of logistics targeting incidents and is designed to be operationally deployable across a range of analyst contexts and evidence environments. The retrospective application of the framework to 94 documented incidents demonstrates its analytical utility and identifies the incident categories — particularly procurement manipulation and human intelligence cultivation — where attribution methodology requires further development. PLIANT's ongoing research program will continue to refine the framework as new incidents are documented and as the evidence base for established attributions is updated through partner intelligence sharing.

References

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Chesney, R., & Smeets, M. (2020). Roundtable on Cyber Conflict. *Texas National Security Review*, 3(1).

Crowdstrike. (2023). *Global Threat Report 2023*. CrowdStrike Inc.

Dempsey, M., & Chertoff, M. (2021). Supply Chain Security and National Competitiveness. *Lawfare*.

Healey, J. (Ed.). (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.

Lindsay, J. R. (2015). Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack. *Journal of Cybersecurity*, 1(1), 53–67.

MITRE Corporation. (2023). ATT&CK for ICS. Retrieved from attack.mitre.org/matrices/ics.

Nakashima, E., & Warrick, J. (2022). Russian Hackers Target U.S. Logistics Networks. *Washington Post*.

PLIANT Institute. (2024). *Atlas Intelligence Database: Annual Program Report*. PLIANT-ATLAS-2024.

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1-2), 4–37.

Torres, M. A. (2023). Nation-State Vectors in Commercial Supply Chain Interference. *PLIANT Working Paper* PLIANT-WP-2023-04.

UNCTAD. (2023). *Review of Maritime Transport 2023*. United Nations Conference on Trade and Development.

Acknowledgments: The author thanks colleagues at PLIANT for feedback on earlier drafts, particularly Dr. S.L. Chen whose Atlas database work provided the empirical foundation for the retrospective incident analysis, and Dr. J. Patterson for guidance on the policy implications section. The author's views reflect his own analysis and not those of any prior employer.

Correspondence: m.torres@projectpliant.com