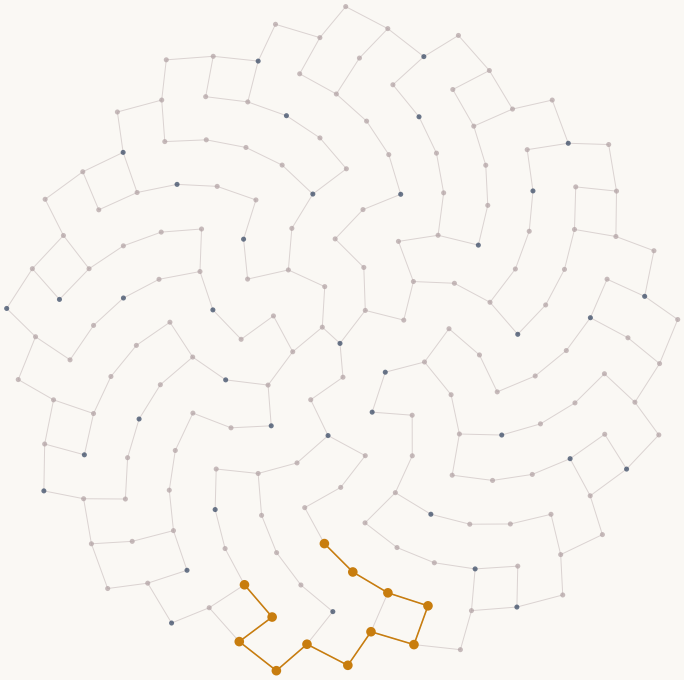

Stopping Sensitive Technology Flows: The Hidden Network Problem

Export controls and licensing are failing.

Adversaries are moving sensitive technology through shell networks. Network visibility is the missing counterproliferation tool.

By Sayari Analyst Team . Published March 2025 . sayari.com

EXPORT CONTROLS

Stopping Sensitive Technology Flows: The Hidden Network Problem

By Sayari Analyst Team · Published March 2025

Export controls and licensing are failing. Adversaries are moving sensitive technology through shell networks. Network visibility is the missing counterproliferation tool.

The Export Administration Regulations (EAR) assumed that listing sensitive technology, licensing transfers, and maintaining entity watchlists would stop adversaries from acquiring it. That model fails today. Sensitive technology reaches adversaries not because the EAR is weak on paper, but because its enforcement is blind: regulators identify restricted technology but cannot reliably see who acquires it. Semiconductors bound for military end-users in sanctioned jurisdictions move through shell corporations across multiple countries, intermediaries, and transshipment hubs. By arrival, the regulatory trail vanishes. The problem is not regulation-it is visibility.

The U.S. Department of Commerce Bureau of Industry and Security launched the Disruptive Technology Strike Force in 2022 to address this gap. Without network-level visibility into corporate structures, ownership chains, and procurement patterns, regulators cannot stop flows. Adversaries move semiconductors, AI systems, quantum research, and biotechnology through networks designed to obscure ownership and end-use. Stopping these flows requires mapping hidden networks and tracing technology from origin to military end-users.

The Regulatory Landscape Has Tightened, But Visibility Hasn't Kept Pace

The EAR controls exports of semiconductors, encryption, biotech equipment, AI models, and quantum components-technologies central to military advantage. The framework distinguishes "dual-use" items (civilian purpose, military capability) from general goods, triggering licensing and entity screening requirements on those designated items.

Over three years, controls intensified: semiconductor restrictions (2022), AI guardrails (2024), biotech controls, and quantum oversight initiatives. Each reflects a reality-technological superiority in semiconductors, AI, and advanced manufacturing underpins military power and industrial competitiveness. Regulators expanded controlled-items lists and penalties for violations, but expanding lists without expanding visibility creates a structural gap. Export control officers rely on end-use statements, customer screening, and destination review-all tools dependent on accurate information from counterparties. When front companies submit false end-use statements, corporate ownership is deliberately obfuscated across secrecy jurisdictions, or distributors unknowingly enable diversion, traditional controls fail. The BIS Entity List captures known bad actors but misses the broader networks through which they acquire technology and the ownership structures that shield them.

The Adversary Playbook: Layers of Legal Concealment

Adversaries move sensitive technology through networks designed to break sight lines between acquirer and regulator. Military end-users rarely appear directly in procurement records. Instead, front companies in weak-disclosure jurisdictions submit purchase orders, often owned by offshore entities extending through multiple jurisdictions with each link providing legal distance from the true end-user. Components travel through multiple hands-a Taiwan semiconductor sells to a Singapore distributor, then to a UAE trading company, then to an adversary end-user. Each step is nominally legal; regulators examining individual transactions miss the patterns. A PLA research institute does not directly purchase from U.S. fabs; a front company bearing a generic name receives goods and diverts them. These companies maintain bank accounts, file taxes, and handle legitimate business alongside diverted procurement. A single regulatory audit finds nothing suspicious. Network analysis revealing dozens of restricted semiconductor shipments routed to military facilities exposes what point-in-time audits miss. Transshipment jurisdictions like Hong Kong, UAE, and Singapore amplify concealment through legitimate commerce, weak beneficial-ownership rules, and geographic proximity to target markets. Adversaries deliberately exploit fragmented regulator visibility across jurisdictions.

The Data Gap

Regulators excel at defining what should not flow but remain blind to what does. The BIS maintains controlled-technology lists and designated entities, but a controlled semiconductor has clear regulatory designation while the shell company that purchases and diverts it remains invisible until caught. Investigators can identify shipment origin and examine export customs records, but lose visibility once items enter global commerce-does it stay in-country or get re-exported? Who owns it at each stage? Does it reach the stated end-user or get diverted? Without visibility into corporate structures and beneficial ownership across jurisdictions, investigators trace individual shipments, not procurement networks. Adversaries deliberately layer jurisdiction, corporate structure, and intermediaries, exploiting fragmented global visibility. Regulators cannot easily see into corporate registries in the UAE, Hong Kong, or secrecy jurisdictions. Trade data, customs information, and corporate ownership records fragment across 250+ jurisdictions, many with no information-sharing agreements with U.S. authorities. A controlled item leaving the United States may pass through five jurisdictions before arriving at its actual end-use location, with each transition obscuring the trail. Network mapping-connecting corporate records, trade flows, and beneficial ownership-reveals hidden procurement networks and links front companies to true owners and end-users.

Shifting to Network-Level Visibility

Counterproliferation requires shifting from transaction-level enforcement to network-level intelligence. The traditional model-identify item, license export, screen end-user, verify compliance-is insufficient. Stopping sensitive technology flows requires identifying hidden networks, mapping corporate structures across jurisdictions, and tracing technology from origin to military end-users. This requires connecting corporate and trade data across sources and jurisdictions: beneficial-ownership information from high-risk registries, trade data showing shipment flows, customs records, and sanctions lists. When integrated, hidden networks become visible. Network visualization enables real-time intervention-investigators visualize ownership chains and identify procurement clusters, tracing components from U.S. origin through intermediaries to end-users, revealing full networks rather than discovering diversions after the fact.

The technical infrastructure exists. Corporate registries maintain beneficial-ownership information increasingly accessible under international standards. Trade databases document flows. The missing piece is integration: pulling sources together, matching entities across jurisdictions, and visualizing networks. When an export control officer investigating a

suspicious shipment sees the claimed end-user is a front company owned by an entity that received a dozen restricted shipments with ownership tracing to a military research institute, enforcement becomes real-time and certain. Agencies equipped with network visibility tools shift from reactive prosecution to proactive prevention, identifying networks before proliferation completes. The adversary playbook depends on fragmentation; network-level counterproliferation flips this. When corporate data connects across jurisdictions, beneficial ownership becomes visible, and trade flows reveal patterns, sensitive technology flows become traceable and hidden networks become exposed.

For organizations tasked with counterproliferation, the path forward is clear: map networks, expose hidden structures, and trace flows. Request a demo of Sayari's Defense Intelligence platform to explore how network visibility transforms counterproliferation strategy and enables real-time enforcement across corporate and trade data.

Please visit sayari.com to learn more.

This blog is for informational purposes and isn't intended to be legal advice.