



The MCF Gap: Why Designation Systems Miss the Majority of the Risk

Fewer than 200 Chinese companies with military-civil fusion ties are formally designated.

Over 1,000 exist. Here's what your screening systems miss. (Source:

CSIS analysis of MCF-designated entities, 2024)

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

GOVERNMENT / EXPORT CONTROLS

The MCF Gap: Why Designation Systems Miss the Majority of the Risk

By Sayari Analyst Team · Published March 2025

Fewer than 200 Chinese companies with military-civil fusion ties are formally designated. Over 1,000 exist. Here's what your screening systems miss. (Source: CSIS analysis of MCF-designated entities, 2024)

You believe the Entity List and related sanctions programs identify the foreign actors you need to know about. You run screening tools. You conduct investment reviews against published designations. The assumption seems safe: if a Chinese company matters for national security, it will eventually appear on a list.

That assumption worked when designations were rare and enforcement reactive. Neither holds now.

In 2024 alone, the U.S. designated 263 Chinese entities through BIS, OFAC, and investment screening—the most active year on record, according to CSIS. Yet researchers tracking Military-Civil Fusion networks identify 1,000-plus Chinese companies with documented MCF ties. Fewer than 200 are formally designated. The gap reveals a structural problem: your screening systems see only what you designate, and designation lags far behind detection.

For federal analysts and policymakers, the implication is unavoidable. Your technology denial mandate depends on designation and investment screening. But these tools cover only 15-20% of the target. For the hundreds of MCF-connected entities not yet designated, your systems are blind.

What the MCF Gap Actually Means

Military-Civil Fusion is policy doctrine, not conjecture. Chinese strategy explicitly mandates state support, talent sharing, and technology transfer between defense research institutes and commercial enterprises. An MCF-connected company is one with documented ties to Chinese military or defense capacity-through shared personnel, subsidiary ownership, research contracts, or investment structures.

The problem: MCF connection is not equivalent to sanctions violation. A company can integrate into China's military supply chain and still operate legally across borders. Visibility depends on which intelligence gets published and when. The BIS Entity List focuses narrowly on export control evasion. OFAC designations follow proven violations. Investment screening through CFIUS/FIRRMA is newer and lags detection by years.

Your formal entity list-your agency's primary tool-captures only MCF companies that have already triggered export violations or financing restrictions. It misses the broader network. Hundreds of MCF-connected entities remain available for technology collaboration, operate in financial markets, and conduct standard business precisely because they are not designated. They are known to intelligence. They are invisible to your systems.

Why Designation Cannot Keep Pace with the MCF Expansion

Designation is case-driven and reactive. Entities get listed when they violate export rules, attempt restricted transactions, or trigger policy action. It is never proactive.

MCF expansion outpaces designation. CSIS documented 263 designations in 2024-a record. But the MCF-connected universe grew simultaneously. Chinese policy pushes deeper civil-military integration, not less. The gap is expanding.

Here is the structural problem: entities remain unknown until caught. They are caught when they violate export rules, apply for U.S. technology, or attempt investment. By then, they have already operated in the U.S. ecosystem, made partnerships, filed licenses, and invested in infrastructure. Designation halts future business but cannot reverse past operations. Other MCF entities continue the same behavior because they understand: risk arrives only through individual designation.

Your screening tools work within this delay. Built to catch designated entities, they will not flag an undocumented MCF company-regardless of how clearly your intelligence analysts know its

military ties. The system is exhaustive within its list. It is blind outside it.

What the MCF Gap Looks Like at Scale

A U.S. semiconductor firm evaluates a materials supplier in Taiwan sourcing inputs from a mainland Chinese chemical company. That company is not on the Entity List, not an OFAC target, and absent from public screening databases. Your agency has no stated position.

But your intelligence colleagues know it. Open-source documentation links it to a PLA research institute through joint research papers. Corporate records show a PLA general on the board. Personnel rosters track transfers to a defense industrial entity. The MCF connection is documented and real.

Under your current regime, that company will not be flagged when the semiconductor firm runs it through compliance screening. CFIUS may trigger—because the acquirer is sensitive—not because the target is known to be MCF-connected. The connection remains invisible.

Multiply across hundreds of entities. Intelligence reports documenting MCF connections exist within your agencies. They do not become actionable policy until formal designation occurs. The entity operates normally in the interim. Because designation is resource-constrained and case-driven, many documented MCF connections never trigger action.

From Detection to Designation: Building the Path Forward

Decoupling MCF intelligence from designation processes is essential. This is not replacing formal lists with unvetted assessments. It means building systematic MCF targeting that precedes designation.

First, build a documented MCF database below the designation threshold. This is operational readiness, not compartmentalization. Analysts at CFIUS, Commerce, and Treasury use separate tools and mandates. An MCF database accessible across agencies transforms screening. Rather than waiting for one agency to designate, all agencies see the same universe of concern.

Second, integrate MCF flagging into screening systems. Export control platforms, investment screening, and sanctions tools must ingest MCF data as an intelligence layer. The screening question shifts: is this entity documented as MCF-connected? Not: is it on the list?

Third, shift designation from reactive to threshold-based. Any MCF-connected entity with ties to sensitive technologies-semiconductors, advanced materials, AI-becomes a designation candidate within a defined period. Designation becomes formalization, not discovery.

Sayari's platform addresses this gap directly. It maintains primary-source corporate structure, ownership, and personnel data across 250+ jurisdictions, including China. Intelligence teams can identify the full MCF universe by linking registry data, research metadata, and ownership chains without waiting for enforcement events. The intelligence question becomes answerable: How many Chinese companies have verifiable MCF connections? Which operate in sensitive sectors? What is their U.S. exposure? See how Sayari supports technology denial missions

The Entity List remains your formal tool. But it cannot be your only detection mechanism. Intelligence-driven MCF targeting at the network level is what makes designation timely, not perpetually reactive.

Please visit sayari.com to learn more.

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