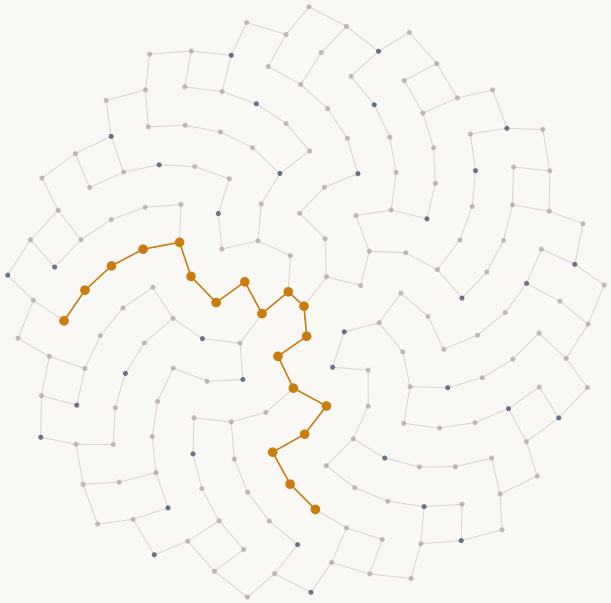

Risk, Regulation, and AI.

Lessons Learned from Frankfurt.

May 6, 2026 . U.S. Consulate General, Frankfurt am Main

IN CASE YOU MISSED IT

Risk, Regulation, and AI: Lessons Learned from Frankfurt

May 6, 2026 . U.S. Consulate General, Frankfurt am Main

Sayari's Frankfurt executive forum convened senior compliance officers, trade counsel, and risk leaders from financial services, manufacturing, technology, and the legal sector for a day of expert dialogue and hands-on analytical demonstration, held at the U.S. Consulate General and opened by the Senior Commercial Officer of the U.S. Department of Commerce.

The event ran two expert panels. One focused on the evolving regulatory landscape for supply chain and sanctions risk. The other on the role of AI and data in enabling compliance at scale. Following these sessions was a technical workshop in which Sayari analysts walked through two live case studies using real platform data.

This summary organises the key takeaways across three themes:

- **The Evolving Risk Landscape.** The EU's 20th sanctions package signals a permanent shift toward OFAC-like enforcement, expanding restrictions on services, naming specific diversion hubs, and converging with U.S. secondary sanctions on Russia, Iran, and China. Organisations must now treat compliance as a strategic function.
- **AI, Data, and the Intelligence Advantage.** General purpose AI tools are insufficient for compliance work, which demands regulatory precision, structured data, and investigative judgement that open-web LLMs cannot reliably provide. Sayari's advantage lies in a decade of formalised tradecraft, enabling organisations to trace complex ownership and trade patterns at scale.
- **Tradecraft in Action: Case Studies.** Sayari's live case studies demonstrated that compliant-looking entities regularly conceal serious exposure. A German hardware reseller with a stated commitment against Russian sales was inadvertently shipping dual-use goods through Central Asian corridors, while an Italian manufacturer's supply chain traced back

through India to a ULPA-listed Xinjiang entity. In both cases, the risk was fully captured in corporate registries and customs data; it simply required the cross-jurisdictional visibility and investigative tradecraft to surface it.

THEME 1 . THE EVOLVING RISK LANDSCAPE

A Sanctions Regime in Transition: EU 20th Package and Secondary Sanctions

The expert consensus was unambiguous: the era of "change through trade" (German: *Wandel durch Handel*) as a guiding philosophy is over in the wake of Russia's invasion of Ukraine.

For thirty years, globalisation was driven by efficiency. That model has fundamentally shifted toward fragmentation where commerce is increasingly defined by national security, regulation, and political alignment. Sanctions are no longer temporary but embedded and evolving. The strategic rivalry between the U.S. and China is intensifying. Russia continues to destabilise global order. Trade is actively weaponised. Evasion networks have grown more adaptive and robust. For organisations operating across these dynamics, risk is no longer visible at the surface level.

A senior trade controls counsel described the EU's 20th sanctions package, released last month, as a deliberate signal that restrictions against Russia will not loosen and that the direction of travel is toward an OFAC-like enforcement posture. Key additions include restrictions on services, not just goods, and named diversion hubs. Kyrgyzstan was called out explicitly as a transshipment corridor of active concern.

The convergence with the US is extending beyond Russia. Iran sanctions were reactivated in September 2025 following suspension under the JCPOA, bringing EU posture into close alignment with American secondary-sanctions practice. Panelists noted that customers are no longer asking "what can I do today?" but are increasingly asking "what will happen tomorrow?" Scenario planning and extraterritorial reach are now core compliance functions.

EU 20TH SANCTIONS PACKAGE

The Direction of Travel

Services restrictions are expanding. Diversion hubs are being flagged by name. The EU is converging toward a de facto secondary-sanctions posture, meaning banks and corporations with indirect exposure to Russia, Iran, and China must now look beyond the face of transactions to understand end-use and ultimate beneficial ownership.

On China: the EU is updating dual-use export controls with a focus on semiconductors and directly sanctioning select Chinese entities, while European companies are simultaneously

facing Chinese export control restrictions imposed in return. The dual-use framework (technically country-neutral) is, in practice, increasingly China-directed. Panelists warned this is not a temporary posture. It is the new baseline.

DUAL-USE GOODS AND CHINA

The Emerging Compliance Frontier

Dual-use restrictions are being updated in real time. Semiconductor controls are the focal point, but the underlying logic extends to any technology with potential military application. European firms face exposure coming from both directions: EU controls on exports to China, and Chinese export restrictions on goods flowing back to Europe.

What Effective Compliance Programs Look Like Today

The fragmentation of the risk landscape (more jurisdictions, more instruments, more obligations) is outpacing point-specific compliance tools. What emerged across both panels was a clear picture of what effective programs have in common. These programs break silos, they speak the board's language, and they treat compliance as a strategic function rather than a reactive one.

One major industrial manufacturer grew its compliance function from two to 150 people in four years after discovering its components in Russian military equipment post-2022. The governance model that emerged is a three-tier defense structure: operational responsibility at the business unit level (first line), structured process and oversight at the compliance function (second line), and a cross-functional compliance committee integrating legal, internal audit, procurement, and finance (third line).

The design principle is not one of centralisation. It is one of breaking silos.

- **Value-based compliance, not just rule-based:** orient around the organisation's purpose, not just the minimum legal standard.
- **Board engagement through storytelling:** real-world enforcement consequences and personal liability exposure land. KPI dashboards alone do not.

- **Compliance as a long-term revenue guarantor:** the balance between compliance and profitability is a false dichotomy. Banks and partners now probe transactions going back a decade (the OFAC/BIS statute of limitations is ten years).
- **Strategic advisory as the future of compliance:** identifying not just risks but opportunities; combining legal with finance, operations, and data analytics in a unified risk function.

THEME 02 . AI, DATA, AND THE INTELLIGENCE ADVANTAGE

The AI Reality Check

The AI panel addressed industry hype, noting that only 5% of companies truly understand AI strategy. Another 35% are progressing without clear direction, while the majority remain unengaged.

Early “bolt-on” tools have failed to yield expected productivity gains. Consequently, focus has shifted toward deep human-AI integration, including “digital twins” and agentic workflows where AI manages structured tasks and humans govern high-stakes decisions.

The identified winning model integrates a robust data layer with an AI-agent layer on top. Traditional SaaS, operating without this structure, is increasingly inadequate. The gap between AI-capable organisations and others is widening, particularly in their ability to handle enforcement scrutiny.

Ground Truth Data: The Non-Negotiable Foundation

Across every AI use case discussed, one constraint surfaced consistently: general-purpose LLMs trained on the open web cannot reliably answer compliance questions that depend on regulatory precision and jurisdictional specificity. One major ERP provider has addressed this by training a dedicated model on actual regulatory text, enabling compliance teams to query restricted goods lists directly and ask what products are restricted under the EU 20th sanctions package, rather than reading thousands of legal pages. The model answers based on verified source material, not probabilistic inference.

A structural limitation was also named directly: AI today handles natural language well but struggles with tables. This shortcoming is a critical gap for compliance, which is fundamentally built on tabular data: sanctions lists, trade manifests, corporate filings, ownership registers. Platforms that serve machine-readable, structured, primary-source data into AI workflows hold a durable advantage over general-purpose tools.

The Sayari Advantage: Tradecraft Formalised at Scale

Sayari framed the critical distinction: assessed intelligence matters more than data volume. Compliance failure is not due to a shortage of data. It is a result of the inability to find the signal in the noise, connect the dots across jurisdictions, and apply investigative judgment to ambiguous structures and trade patterns.

Data does not make decisions. Technology does not make decisions. People do. What Sayari has built over eleven years is not just data or software. It is tradecraft, the ability to interpret complex, imperfect information and make defensible, explainable decisions. Using AI, that tradecraft is now being operationalised at scale, giving organisations access to analytical judgement around the clock. The need for transparency and judgment into global supply chains, and for understanding who we are truly doing business with, is more a necessity than ever.

BEYOND THE GENERIC CHATBOT

Ground truth matters.

A general-purpose AI model trained on the open web cannot trace a multi-tier corporate ownership chain through Chinese provincial registries, identify a Kyrgyz transshipment entity by its trade flow pattern, or surface a German GmbH as a subsidiary of a state-owned defence contractor. Sayari brings a decade of analytical, investigative, and practitioner tradecraft, formalised into automated workflows that apply structured judgment at scale. Verified primary-source data (corporate registries, customs bills of lading, sanctions designations) combined with the investigative expertise to interpret it is the only foundation that holds up under regulatory scrutiny.

A direct caution followed. Bad actors are adopting the same AI tools at the same pace as compliance teams. There is no built-in defensive advantage to AI adoption alone. The answer is better AI built on better data, structured by genuine investigative expertise, not automation layered over an information deficit.

THEME 03 . TRADECRAFT IN ACTION: CASE STUDIES

Sayari's analysts demonstrated two live cases using Sayari's platform, each designed to show what structured trade and corporate data reveals when applied with investigative depth. A case focused on Russia traced a multi-layered sanctions evasion network from a single compliant-looking German entity. A China case showed how forced labour, military end-use, and state-ownership exposure are embedded in supply chains that screen clean at the surface level.

Case Study 1: Russia Sanctions Evasion Network

In the first example, a German computer consultancy and hardware reseller is not flagged for sanctions or adverse media findings. Its website carries a prominent "No Russia" clause citing EU Regulation 833/2014. On a due diligence form, it is a compliant exporter.

But trade data, available via Sayari, tells a different story.

432

DIRECT SHIPMENTS TO RUSSIA (2019-2023)

91% of total outbound volume

1,108

SHIPMENTS VIA TURKEY CORRIDOR

Ervacan Makina (6 sanctions designations), onward to Russia

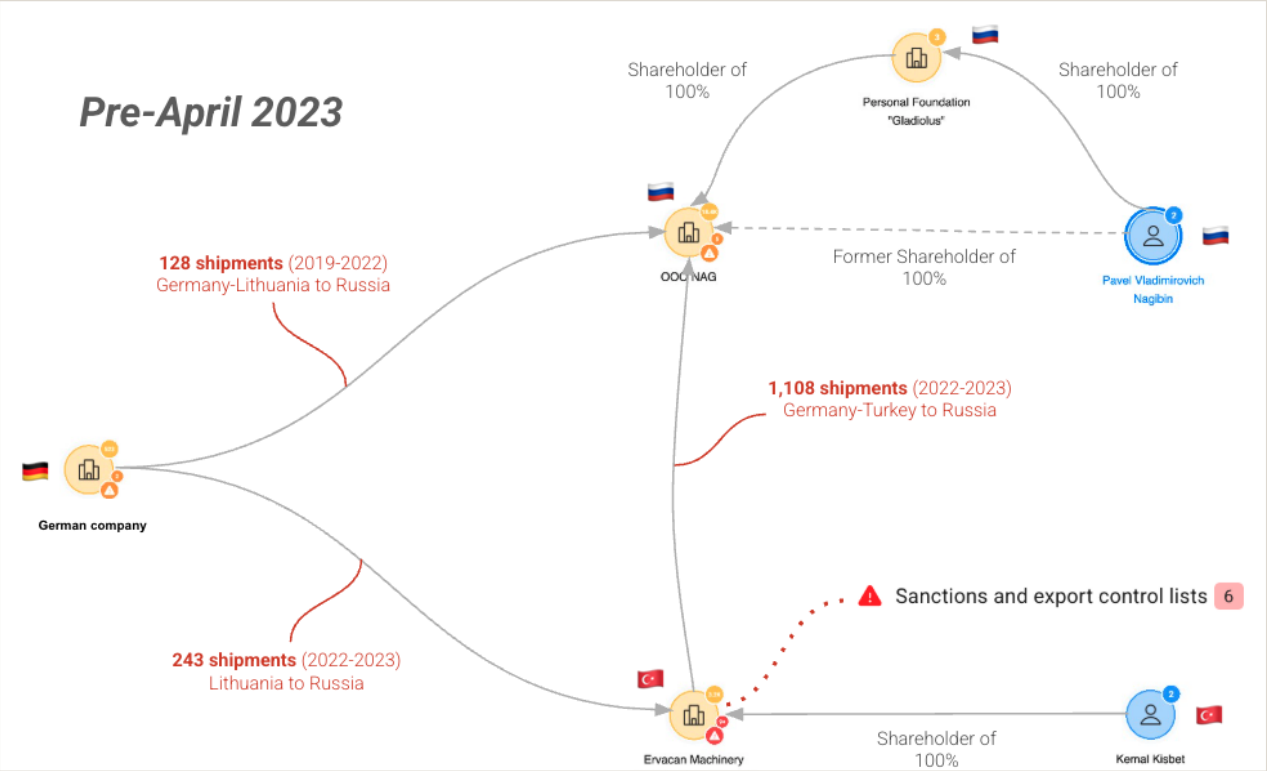

Fig. 1: Cybertrading GmbH — trade flow network, 2019–2023

Before April 2023, the company was involved in direct shipments from Germany to Russia via Lithuania alongside shipments sent via a Turkish intermediary with six sanctions designations acting as a pass-through to the ultimate destination of Russia.

These shipments did not involve generic IT supplies. They involved products included on the Common High Priority Items List, which encompasses technology that Moscow urgently seeks for military and defence purposes. Under EU Regulation 833/2014 Annexes VII and XI, every post-2022 shipment of this product category could be an export violation.

Related payments from Turkey to Germany might look like routine B2B hardware transactions. The Russia connection is only visible when both legs of the trade are viewed simultaneously.

Then, enforcement pressure grew.

LEGAL NOTE

The No-Russia Clause Is Evidence, Not a Shield

EU Regulation 833/2014 places the export prohibition on the exporter, not the buyer. A contractual no-Russia clause cannot transfer that regulatory obligation downstream. What the clause does do is document the seller's knowledge of the prohibition. Under Germany's Foreign Trade and Payments Act §17, knowingly violating an embargo carries up to ten years' imprisonment. The clause is not a compliance defense.

In March 2023, trade corridors shifted to include a new Uzbekistan corridor (two weeks before the Russia channel closes). In June, a Kazakh subsidiary of the Russian distribution network opened a new procurement channel. In December, a second Uzbek entity became active. And in September, a new Kazakh company was registered; it began shipping in February of 2025.

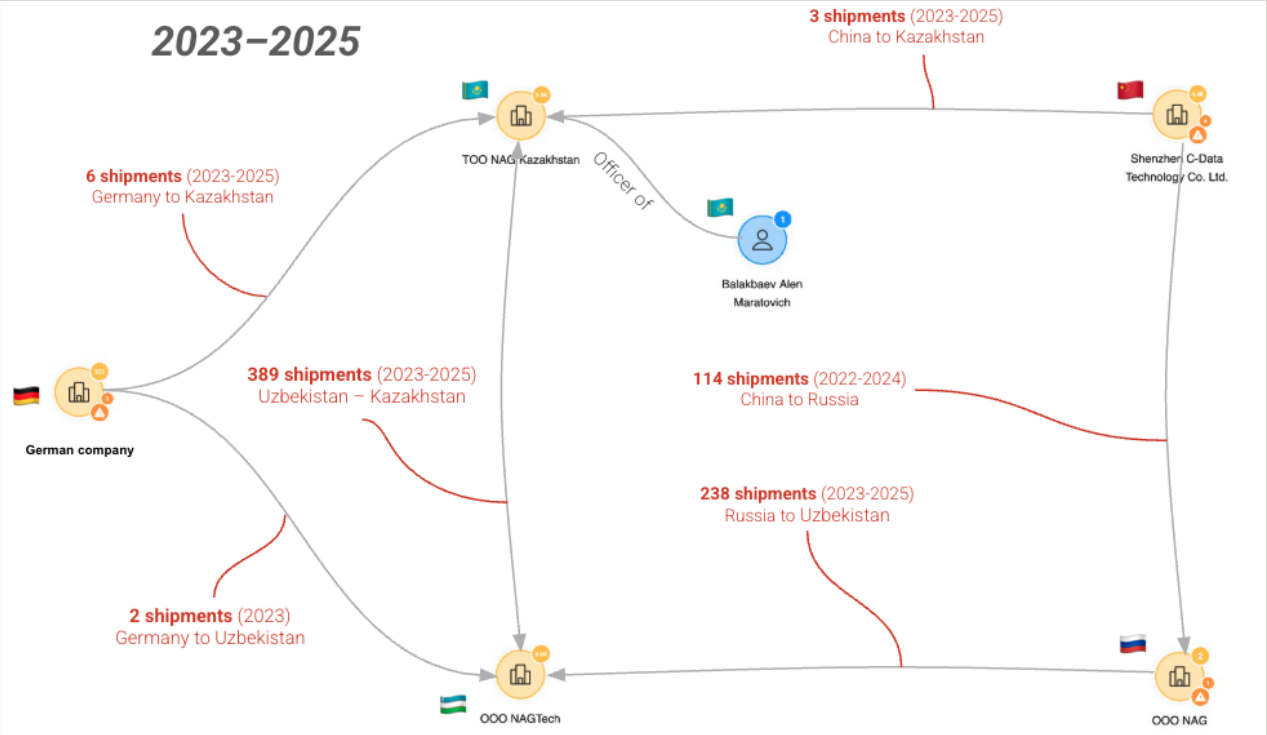

Fig. 2: Corridor shift timeline, 2023–2025

There were six months or fewer between each closure and each opening. These corridors were pre-positioned. The compliance pressure closed one door, and the network opened three more, all with Kazakhstani or Uzbek registrations, all with payments in EUR through Central Asian correspondent chains, none showing Russia on the face of the transaction.

The entity at the center of the pivot, TOO NAG Kazakhstan, revealed its own purpose publicly. At a 2022 Kazakhstani telecommunications conference, a company representative stated on camera that the company was the “first representative of the NAG company outside of Russia,” confirming it was not an independent Kazakh distributor. It was an extension of a Russian illicit procurement network, established before sanctions to sustain acquisition of sensitive goods.

Case Study 2: Forced Labour, Military End-Use, and SOEs in Germany

The second case addresses structural rather than network risk, specifically, compliance exposure embedded in supply chains that appear clean at the entity level. The entry point is an Italian manufacturer of aluminium electrolytic capacitors (components used in industrial power systems, EV battery management, and defence electronics) with sales representation in Germany. Trace the supply chain upstream three tiers and the picture changes completely.

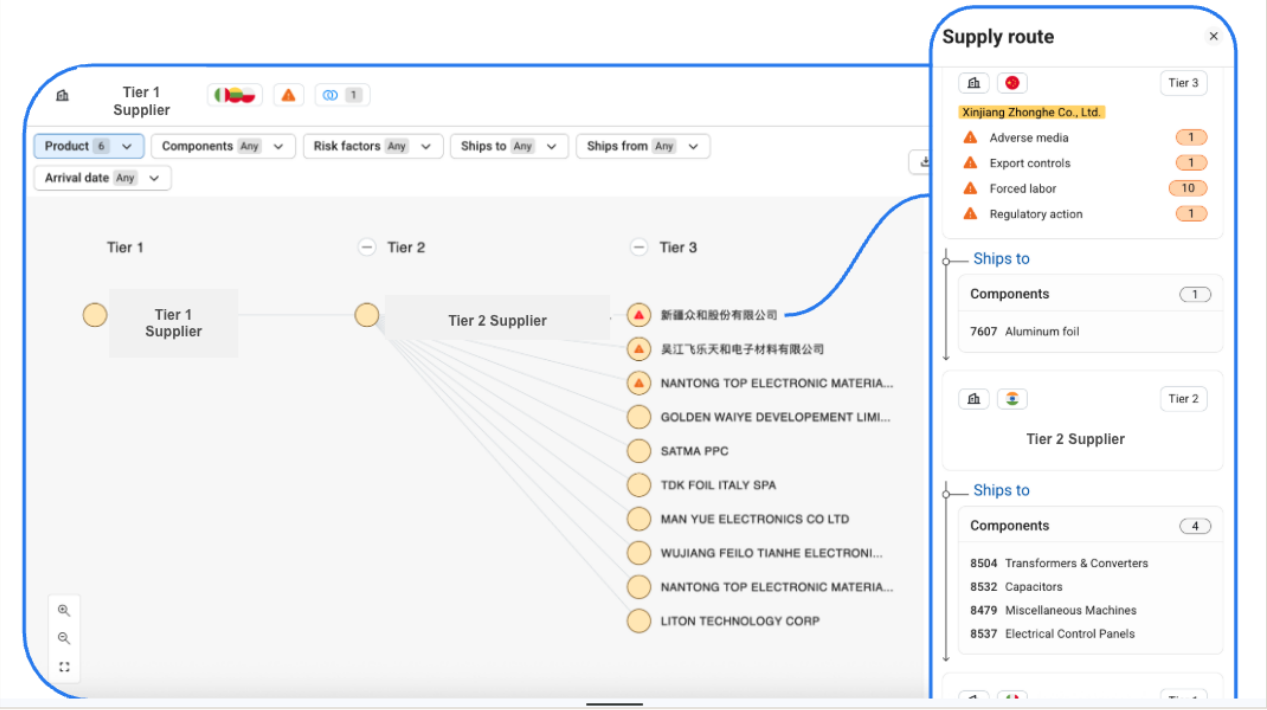

Fig. 3: Sayari supply chain visualisation of Italian company's upstream supply chain — Italy–India–Xinjiang

TIER	COUNTRY	ENTITY
TIER 1	**Italy**	Italian manufacturer. Screens clean at entity level.
TIER 2	**India**	Indian manufacturing subsidiary. Sources aluminium foil inputs.
TIER 3	**Xinjiang, China**	Xinjiang Joinworld (UFLPA-listed, XPCC contractor). 30 direct shipments named in Italian customs records.

This is documented in customs bills of lading, not inferred. Thirty direct shipments from a US-government designated forced labour entity arrived in Italian customs records. The Italian manufacturer's bank relationships, letters of credit, and trade finance structures are potentially connected to that chain.

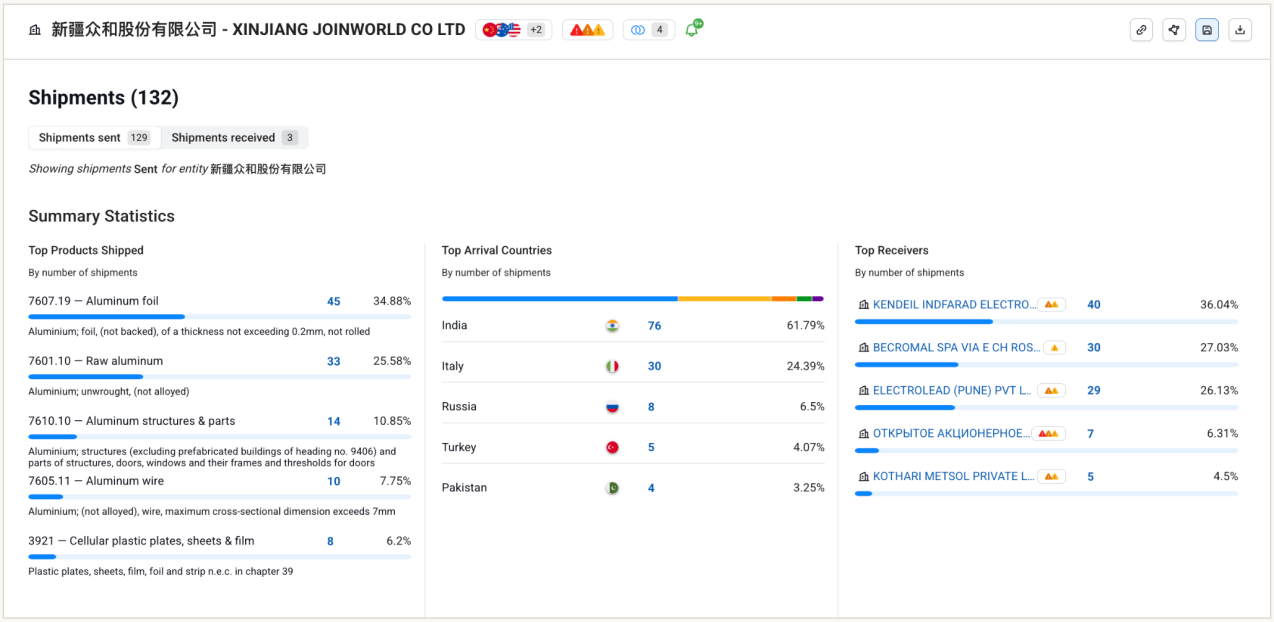

Fig. 4: Trade flow documentation — Xinjiang to Italy

UFLPA

The Burden-of-Proof Standard

The US Uyghur Forced Labor Prevention Act establishes a rebuttable presumption: goods from listed entities are presumed to involve forced labour unless the importer proves otherwise. For banks financing those imports via letters of credit, the compliance exposure is direct. The EU Forced Labour Regulation (2024/3015), which has been in force since December 2024, provides for import bans. Overhauling due diligence processes often takes years, meaning that mandatory implementation across the EU from December 2027 is just around the corner.

The exposure compounds at the subsidiary level. The listed Xinjiang entity's corporate network includes eleven downstream subsidiaries, each carrying a forced labour risk flag in Sayari data. But one stands out for an entirely different reason. Its official business registration, filed with Chinese state authorities, discloses a business purpose that includes research and development of rocket launch equipment and manufacturing of military equipment supplies.

This is not from an intelligence report. It is what the company filed with the Chinese government for its own purpose, all captured by Sayari, which reads Chinese corporate registry data at source.

The ownership chain runs from that entity through a state-controlled provincial holding company to the Sichuan Provincial Government's SASAC, a state-backed management mechanism that ultimately links to the Chinese State Council. A UFLPA-listed forced labour entity has a subsidiary registered for weapons manufacturing, controlled by the Chinese state. That sits in the supply chain of companies with European banking relationships.

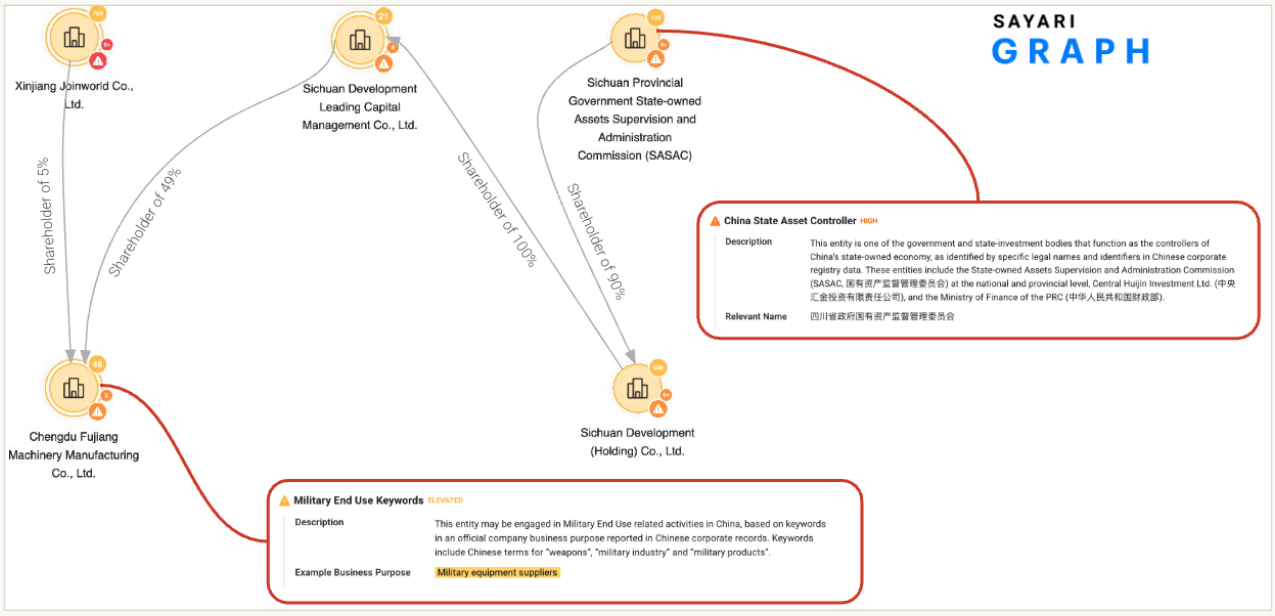

Fig. 5: Ownership chain — Xinjiang entity to Chinese State Council

CASIC

Subsidiaries Registered in the German Handelsregister

China Aerospace Science and Industry Corporation (CASIC) is 100% state-owned by China's State Council and named on the US NDAA Section 1260H Military-Industrial Complex list. It is also the ultimate beneficial owner of at least three GmbHs currently registered in Germany identified by Sayari. A standard Handelsregister search returns German companies. It does not return CASIC. That link is only visible through cross-registry ownership tracing: German filings connected to Chinese state corporate data. The German Money Laundering Act §10 requires enhanced due diligence where the beneficial owner chain runs to a state-controlled entity. BaFin's §44 examination focus for 2025 includes Chinese client portfolios. The gap between what a standard KYC check finds and what the data actually shows is auditable. And examiners are looking.

The throughline across both case studies is that the risk is in the data. Corporate registries hold it. Trade manifests name it. What has been missing is the infrastructure to connect those sources across jurisdictions and the investigative discipline to interpret what they reveal at the speed and scale modern compliance demands.

THE QUESTION THAT CLOSES EVERY CONVERSATION

When the examiner asks how your firm identified the beneficial owner of its Chinese GmbH clients, or how your transaction monitoring detected CIS proxy payments for Russian technology acquisition, what is your answer?

ABOUT SAYARI

Sayari is the judgment infrastructure for trustworthy AI in economic security and commercial risk.

The Sayari Commercial World Model resolves 11.7B+ primary-source records from 250+ jurisdictions, forming the ground truth of global commerce. A Judgment Ontology, encoding over a decade of investigative tradecraft, and Superconductor, an agentic orchestration platform, deliver AI that reasons like an expert analyst, shows its work, and traces every finding to its source.

Trusted by regulators and the regulated alike, Sayari is used by U.S. Customs and Border Protection, the U.S. Treasury, Fortune 500 enterprises, and thousands of professionals across 35+ countries to secure supply chains, surface sanctions evasion and forced labor risks, and dismantle illicit networks at scale.

In a volatile geopolitical and regulatory landscape, defenders of the global commercial system need more than monitoring — they need evidence, explainability, and speed. Sayari delivers all three.

Headquartered in Washington, D.C.

sayari.com

DISCLAIMER