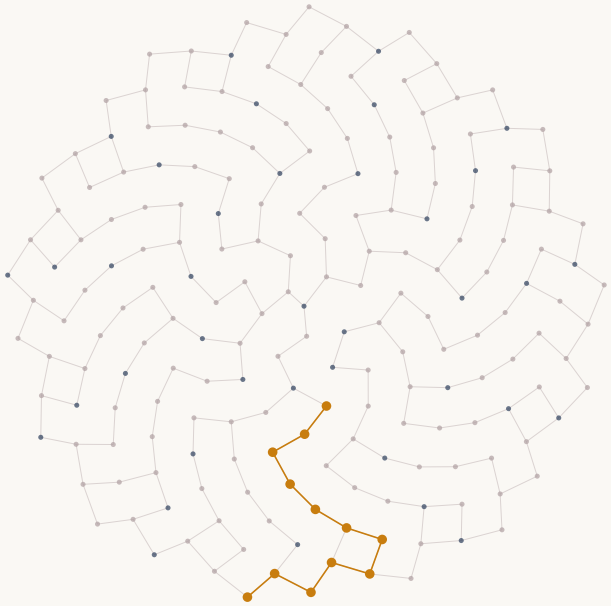

Risiko, Regulierung und KI.

Erkenntnisse aus Frankfurt.

6. Mai 2026 . US-Generalkonsulat, Frankfurt am Main

FALLS SIE ES VERPASST HABEN

Risiko, Regulierung und KI: Erkenntnisse aus Frankfurt

6. Mai 2026 . US-Generalkonsulat, Frankfurt am Main

Sayaris Executive Forum brachte leitende Compliance-Beauftragte, Risikomanager und Juristen aus den Bereichen Finanzdienstleistungen, Fertigung, Technologie und dem Rechtswesen zu einem Tag voller Fachgespräche und praktischer Vorführungen zusammen. Die Veranstaltung fand im US-Generalkonsulat statt und wurde vom Senior Commercial Officer des U.S. Department of Commerce eröffnet.

Im Rahmen der Veranstaltung fanden zwei Experten-Panels statt. Eines befasste sich mit den sich wandelnden regulatorischen Rahmenbedingungen für Sanktionen und Lieferkettenrisiken. Das zweite widmete sich der Rolle von KI und Daten bei der Umsetzung von skalierbarer Compliance. Im Anschluss an die Panels folgte ein Fachworkshop, in dem Analysten von Sayari zwei Fallstudien vorstellten.

In dieser Zusammenfassung sind die Erkenntnisse nach drei Themengebieten gegliedert:

- **Wandelnde Risikolandschaft.** Das 20. Sanktionspaket der EU signalisiert eine Wendung zu einer OFAC-ähnlichen Rechtsdurchsetzung, wobei Beschränkungen für Dienstleistungen ausgeweitet, Umschlagplätze benannt und eine Annäherung an die Sekundärsanktionen der USA gegen Russland, Iran und China erwirkt werden. Unternehmen müssen Compliance nun als strategische Funktion betrachten.
- **KI, Daten und der Intelligenz-Vorteil.** Generische KI-Tools reichen für die Compliance-Arbeit nicht aus, da diese regulatorische Präzision, strukturierte Daten und investigatives Urteilsvermögen erfordert; Fähigkeiten, die open-source LLMs nicht zuverlässig bieten können. Der Vorteil von Sayari liegt in einem Jahrzehnt formalisierter Fachkompetenz, die es Unternehmen ermöglicht, komplexe Eigentums- und Handelsmuster in großem Maßstab nachzuvollziehen.

- **Praktische Anwendung: Fallstudien.** Unternehmen, die den Anschein erwecken, Vorschriften einzuhalten, verbergen oft erhebliche Risiken. Ein deutscher Hardware-Händler, der sich öffentlich gegen Russland positionierte, versandte Dual-Use Güter über zentralasiatische Korridore, während die Lieferkette eines italienischen Herstellers über Indien zu einem in der ULPA-Liste aufgeführten Unternehmen in Xinjiang zurückverfolgt werden konnte. In beiden Fällen waren diese Risiken in Unternehmensregistern und Zolldaten erfasst; es bedurfte lediglich einer länderübergreifenden Ermittlung, um sie aufzudecken.

THEMA 1 . WANDELNDE RISIKOLANDSCHAFT

Sanktionsregimes im Wandel: 20. EU-Sanktionspaket und Sekundärsanktionen

Der Konsens unter den Experten war eindeutig: Die Ära von „Wandel durch Handel“ als Leitideologie ist nach dem Einmarsch Russlands in die Ukraine vorbei.

30 Jahre lang wurde die Globalisierung von Effizienzbestrebungen angetrieben. Dieses Modell hat sich grundlegend in Richtung Fragmentierung verschoben, wobei der Handel zunehmend von nationaler Sicherheit, Regulierung und politischer Ausrichtung bestimmt wird. Sanktionen sind nicht mehr nur vorübergehend, sondern fest verankert und dynamisch. Die strategische Rivalität zwischen den USA und China verschärft sich. Russland destabilisiert weiterhin die globale Ordnung. Der Handel wird aktiv als Waffe eingesetzt. Netzwerke zu Sanktionsumgehungen sind anpassungsfähiger und robuster geworden. Für Organisationen sind Risiken nicht mehr auf den ersten Blick erkennbar.

Ein leitender Außenhandelsjurist bezeichnete das 20. Sanktionspaket als bewusstes Signal, dass die Restriktionen gegen Russland nicht gelockert werden und dass die Entwicklung in Richtung eines OFAC-ähnlichen Enforcement geht. Zu den wichtigsten Neuerungen zählen Beschränkungen nicht nur für Waren, sondern auch für Dienstleistungen sowie explizit benannte Umschlagplätze. Kirgisistan wurde ausdrücklich als Umschlagkorridor genannt.

Die Annäherung an die USA geht über Russland hinaus. Die Iran-Sanktionen wurden im September 2025 nach ihrer Aussetzung im Rahmen des JCPOA wieder in Kraft gesetzt. Die Teilnehmer stellten fest, dass Kunden nicht mehr fragen: „Was kann ich heute tun?“, sondern zunehmend: „Was wird morgen passieren?“ Szenarioplanung und extraterritoriale Reichweite sind nun zentrale Aufgaben des Compliance-Bereichs.

20. SANKTIONSPAKET

Fahrtrichtung des Pakets

Die Beschränkungen für Dienstleistungen werden ausgeweitet. Umschlagplätze werden namentlich benannt. Die EU bewegt sich zunehmend auf eine De-facto-Haltung in Bezug auf Sekundärsanktionen zu, was bedeutet, dass Banken und Unternehmen mit indirekten Geschäftsbeziehungen zu Russland, Iran und China nun über die direkte Transaktionsdimension hinausblicken müssen, um Endverwendungszwecke und die wirtschaftlich Berechtigte zu ermitteln.

Zum Thema China: Die EU aktualisiert derzeit ihre Ausfuhrkontrollen für Dual-Use Güter mit Schwerpunkt auf Halbleitern und verhängt direkte Sanktionen gegen bestimmte chinesische Unternehmen, während europäische Unternehmen gleichzeitig mit chinesischen Ausfuhrbeschränkungen konfrontiert sind, die als Vergeltungsmaßnahme verhängt wurden. Der Rahmen für Dual-Use Güter (der eigentlich länderneutral ist) richtet sich in der Praxis zunehmend gegen China. Die Teilnehmer warnten, dass dies keine vorübergehende Haltung sei. Es handele sich vielmehr um die neue Ausgangsbasis.

DUAL-USE GÜTER UND CHINA

Die neue Compliance-Herausforderung

Die Beschränkungen für Dual-Use Güter werden in Echtzeit aktualisiert. Im Mittelpunkt stehen zwar Kontrollen für Halbleiter, doch die zugrunde liegende Logik erstreckt sich auf jede Technologie mit militärischer Anwendbarkeit. Europäische Unternehmen sind von beiden Seiten betroffen: von den EU-Ausfuhrkontrollen für China und von den chinesischen Ausfuhrbeschränkungen.

Wie wirksame Compliance-Programme heute aussehen

Die Fragmentierung der Risikolandschaft (mehr Gerichtsbarkeiten, mehr Instrumente, mehr Verpflichtungen) schreitet schneller voran als die Entwicklung spezialisierter Compliance-Tools. In beiden Podiumsdiskussionen zeichnete sich ein klares Bild davon ab, was wirksame Programme gemeinsam haben: Sie überwinden Silos, sprechen die Sprache des Vorstands und betrachten Compliance als strategische und nicht als reaktive Funktion.

Ein Industriekonzern baute z.B. seine Compliance-Abteilung innerhalb weniger Jahre auf 150 Mitarbeiter aus, nachdem festgestellt worden war, dass seine Komponenten nach 2022 in russischer Militärausrüstung verbaut worden waren. Das daraus resultierende Governance-Modell ist eine dreistufige Kontrollstruktur: operative Verantwortung auf Ebene der Geschäftsbereiche, strukturierte Prozesse und Aufsicht durch die Compliance-Abteilung sowie ein funktionsübergreifender Compliance-Ausschuss, der die Bereiche Recht, interne Revision, Beschaffung und Finanzen vereint.

Das Grundprinzip besteht nicht in der Zentralisierung, sondern darin, Silos aufzubrechen.

- **Wertorientierte statt rein regelbasierter Compliance:** Sich am Zweck der Organisation orientieren, nicht nur am gesetzlichen Mindeststandard.
- **Einbindung des Vorstands durch Storytelling:** Die Konsequenzen bei der Durchsetzung und das persönliche Haftungsrisiko. KPI-Dashboards reichen nicht.
- **Compliance als Garant für langfristige Rentabilität:** Das Gleichgewicht zwischen Compliance und Rentabilität ist ein Scheingegensatz. Banken prüfen Transaktionen, die bis zu 10 Jahre zurückliegen (die OFAC/BIS Verjährungsfrist beträgt 10 Jahre).
- **Strategische Beratung als Zukunft der Compliance:** Nicht nur Risiken, sondern auch Chancen zu erkennen; die Bereiche Recht, Finanzen, Betrieb und Datenanalyse in einer einheitlichen Risikofunktion zu vereinen.

THEMA 02 . KI, DATEN UND DER INTELLIGENZVORTEIL

Der KI-Realitätscheck

Die Podiumsdiskussion zum Thema KI befasste sich mit dem Hype in der Branche und stellte fest, dass nur 5% der Unternehmen die KI-Strategie wirklich verstehen. Weitere 35% gehen ohne klare Ausrichtung vor, während die Mehrheit noch nicht wirklich aktiv ist.

Frühe „Bolt-on"-Tools haben nicht zu den erwarteten Produktivitätssteigerungen geführt. Infolgedessen hat sich der Fokus auf eine tiefgreifende Integration von Mensch und KI verlagert, einschließlich „Digital Twins" und agentenbasierter Arbeitsabläufe, bei denen KI strukturierte Aufgaben übernimmt, während Menschen Entscheidungen treffen.

Solche Modelle verbinden eine robuste Datenebene mit KI-Agenten. Herkömmliche SaaS-Lösungen, die ohne diese Struktur auskommen, erweisen sich zunehmend als unzureichend. Die Kluft zwischen KI-fähigen Unternehmen und anderen vergrößert sich, insbesondere hinsichtlich ihrer Fähigkeit, behördlichen Kontrollen standzuhalten.

„Ground-Truth"-Daten: Die unverzichtbare Grundlage

Bei allen besprochenen Anwendungsfällen der KI zeigte sich immer wieder dieselbe Einschränkung: Allzweck-LLMs können Compliance-Fragen, die von regulatorischer Präzision und rechtsräumlicher Spezifität abhängen, nicht zuverlässig beantworten. Ein großer ERP-Anbieter geht dieses Problem an, indem er ein Modell auf der Grundlage von Gesetzestexten trainiert hat. Dadurch können Compliance-Teams direkt Listen mit beschränkten Gütern abfragen und sehen, welche Produkte z.B. im Rahmen des 20. Sanktionspakets Beschränkungen unterliegen, anstatt Tausende Seiten durchlesen zu müssen. Das Modell antwortet auf der Grundlage verifizierter Quellen und nicht anhand probabilistischer Schlussfolgerungen.

Eine strukturelle Einschränkung wurde ebenfalls angesprochen: KI kommt heute zwar gut mit natürlicher Sprache zurecht, hat jedoch Schwierigkeiten mit Tabellen. Dieser Mangel stellt eine Lücke für die Compliance dar, die auch auf solchen Daten basiert: Sanktionslisten, Handelsmanifeste, Unternehmensunterlagen, Eigentümerverzeichnisse. Plattformen, die maschinenlesbare, strukturierte Daten aus Primärquellen in KI-Workflows einspeisen, haben einen dauerhaften Vorteil.

Der Sayari-Vorteil: Systematisierte Fachkompetenz in großem Maßstab

Sayari brachte den entscheidenden Unterschied auf den Punkt: Ausgewertete Informationen sind wichtiger als die Datenmenge. Verstöße gegen Compliance-Vorschriften sind nicht auf einen Mangel an Daten zurückzuführen. Sie sind vielmehr das Ergebnis der Unfähigkeit, das Wesentliche aus der Flut von Informationen herauszufiltern, Zusammenhänge über verschiedene Gerichtsbarkeiten hinweg zu erkennen und bei unklaren Strukturen und Handelsmustern ein Ermittlungsurteil anzustellen.

Daten treffen keine Entscheidungen. Technologie trifft keine Entscheidungen. Menschen treffen sie. Was Sayari in elf Jahren aufgebaut hat, sind nicht nur Daten oder Software. Es ist Fachkompetenz; die Fähigkeit, komplexe Informationen zu interpretieren und fundierte, revisionssichere Entscheidungen zu treffen. Mithilfe von KI wird diese Fachkompetenz nun in großem Maßstab umgesetzt, sodass Unternehmen rund um die Uhr auf analytische Einschätzungen zugreifen können. Der Bedarf an Transparenz und Urteilsvermögen in globalen Lieferketten sowie das Verständnis dafür, mit wem wir tatsächlich Geschäfte machen, ist heute wichtiger denn je.

MEHR ALS NUR GENERISCHE CHATBOTS

Die tatsächlichen Gegebenheiten sind entscheidend.

Ein Allzweck-KI-Modell ist nicht in der Lage, mehrstufige Unternehmensbeteiligungsstrukturen anhand chinesischer Provinzregister nachzuvollziehen, ein kirgisisches Umschlagunternehmen anhand seiner Handelsströme zu identifizieren oder eine deutsche GmbH als Tochter eines staatlichen Rüstungsunternehmens aufzudecken. Sayari vereint ein Jahrzehnt an Erfahrung in den Bereichen Analyse, Recherche und praktischer Arbeit und hat diese in automatisierte Arbeitsabläufe umgesetzt, die strukturierte und skalierbare Entscheidungen zu ermöglichen. Verifizierte Daten aus Primärquellen (Handelsregister, Zollfrachtbriefe, Sanktionslisten) in Verbindung mit der investigativen Expertise zu ihrer Auswertung bilden die Grundlage, die behördlichen Überprüfung standhält.

Es folgte eine direkte Warnung. Kriminelle nutzen dieselben KI-Tools im gleichen Tempo wie Compliance-Teams. Die Einführung von KI allein bietet keinen automatischen Vorteil. Die Lösung liegt in besseren Modellen, die auf besseren Daten basieren und durch echte Erfahrung strukturiert werden; nicht in einer Automatisierung, die einen Mangel an Informationen überdeckt.

THEMA 03 . TRADECRAFT IN DER PRAXIS: FALLSTUDIEN

Die Sayari-Analysten stellten zwei Fallbeispiele vor, die verdeutlichen, welche Erkenntnisse strukturierte Handels- und Unternehmensdaten liefern, wenn sie mit investigativer Tiefe ausgewertet werden. Ein Fallbeispiel mit Schwerpunkt auf Russland deckte ein vielschichtiges Netzwerk zu Sanktionsumgehungen auf, das von einem einzelnen, vordergründig regelkonformen deutschen Unternehmen ausging. Ein Fallbeispiel aus China zeigte, wie Zwangsarbeit, militärische Endverwendung und staatliche Beteiligungen in Lieferketten eingebettet sind, die oberflächlich betrachtet keine Auffälligkeiten aufweisen.

Fallstudie 1: Netzwerk zur Umgehung der Russland-Sanktionen

Im ersten Beispiel wird ein deutscher Hardware-Händler weder mit Sanktionen noch mit negativen Medienberichten in Verbindung gebracht. Auf seiner Website ist eine deutlich sichtbare „No Russia“-Klausel zu finden. In einer Due-Diligence-Erklärung wird das Unternehmen als vorschriftsmäßiger Exporteur aufgeführt.

Die über Sayari verfügbaren Handelsdaten zeichnen jedoch ein anderes Bild.

432

DIREKTLIEFERUNGEN NACH RUSSLAND (2019–2023)

91 % des gesamten Exportvolumens

1.108

EXPORTE ÜBER DEN TÜRKEI-KORRIDOR

Ervacan Makina (6 Sanktionsvermerke), weiter nach Russland

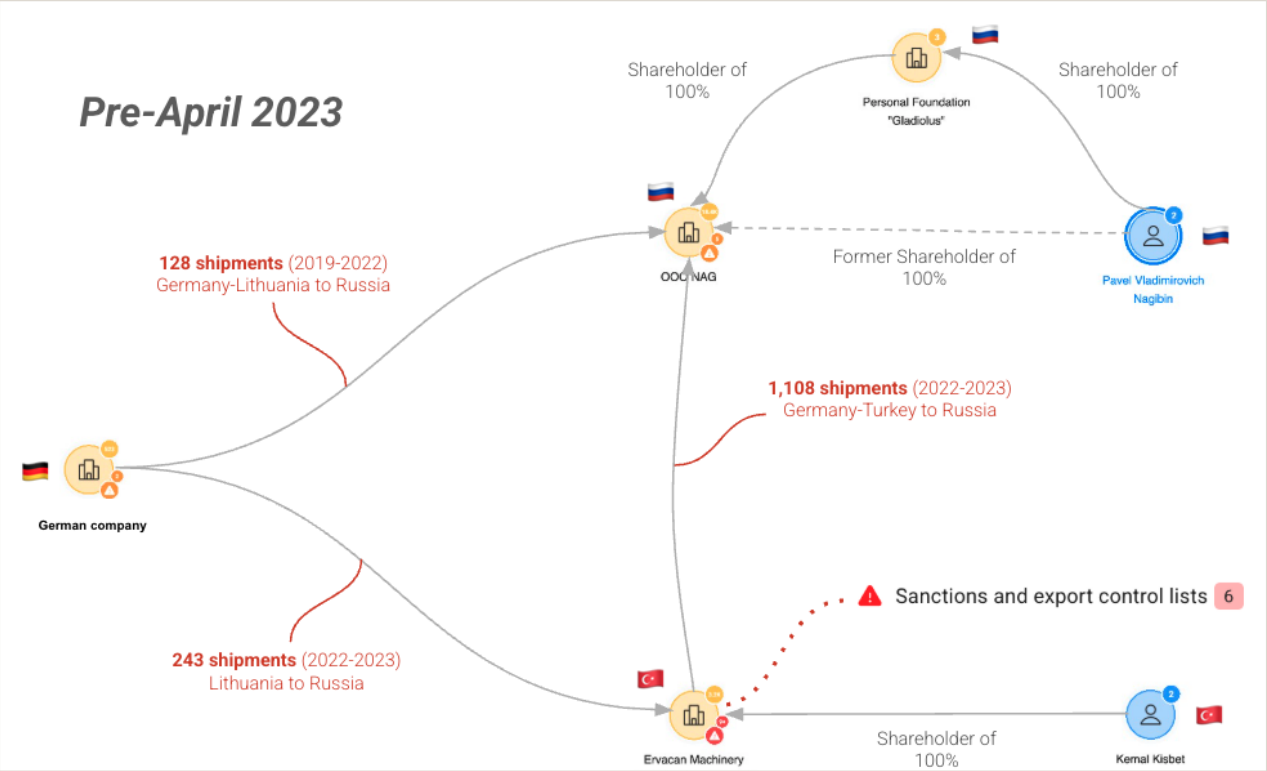

Abb. 1: Cybertrading GmbH: Handelsnetzwerk, 2019–2023

Vor April 2023 war das Unternehmen an Direktlieferungen von Deutschland nach Russland beteiligt sowie an Exporten, die über einen türkischen Zwischenhändler mit sechs Sanktionsvermerken als Umschlagplatz zum Endziel Russland abgewickelt wurden.

Bei diesen Lieferungen handelte es sich nicht um allgemeine IT-Ausrüstung. Es handelte sich vielmehr um Produkte, die auf der CHPL-Liste aufgeführt sind, welche Technologien umfasst, die Moskau für militärische und Verteidigungszwecke benötigt. Gemäß den Anhängen VII und XI der EU-Verordnung 833/2014 könnte jede Lieferung dieser Produktkategorie nach 2022 einen Verstoß gegen die Ausfuhrbestimmungen darstellen.

Entsprechende Zahlungen von der Türkei nach Deutschland könnten wie gewöhnliche B2B-Hardware-Transaktionen aussehen. Der Bezug zu Russland wird erst sichtbar, wenn beide Seiten gleichzeitig betrachtet werden.

Dann nahm der Druck zur Durchsetzung zu.

HINWEIS

„No-Russia“-Klauseln sind Beweise, keine Schutzschilder

Die EU-Verordnung 833/2014 legt das Ausfuhrverbot dem Exporteur auf, nicht dem Käufer. Eine vertragliche „No-Russia“-Klausel kann diese gesetzliche Verpflichtung nicht auf nachgelagerte Parteien übertragen. Die Klausel dient dazu, die Kenntnis des Verkäufers von dem Verbot zu dokumentieren. Nach § 17 des deutschen Außenwirtschaftsgesetzes (AWG) wird die wissentliche Verletzung eines Embargos mit einer Freiheitsstrafe von bis zu zehn Jahren geahndet.

Im März 2023 wurden diese Korridore um einen neuen Handelskorridor nach Usbekistan erweitert. Im Juni eröffnete eine kasachische Tochtergesellschaft des russischen Vertriebsnetzes einen neuen Beschaffungskorridor. Im Dezember nahm ein usbekisches Unternehmen seine Tätigkeit auf. Und im September wurde ein neues kasachisches Unternehmen registriert, das im Februar 2025 mit dem Versand begann.

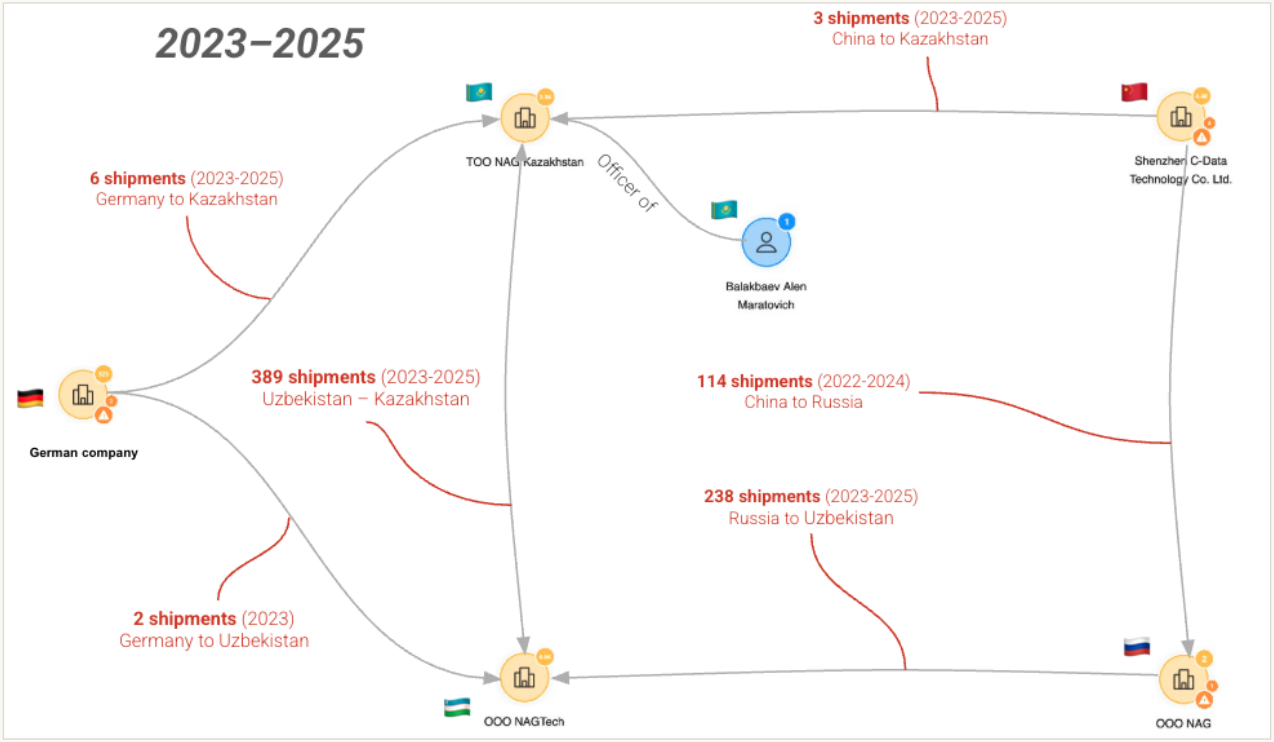

Abb. 2: Zeitplan für die Korridorverlagerung, 2023–2025

Zwischen jeder Schließung und Eröffnung lagen höchstens sechs Monate. Diese Korridore waren bereits im Vorfeld eingerichtet worden. Der Druck zur Einhaltung der Vorschriften führte zur Schließung eines Korridors, doch es öffneten sich drei weitere; alle mit kasachischen oder

usbekischen Registrierungen, alle mit Zahlungen in Euro über zentralasiatische Korrespondenzbanken, wobei Russland in keiner der Transaktionen als Absender oder Empfänger auftauchte.

Das Unternehmen im Zentrum dieser Machenschaften gab seine eigentliche Zielsetzung öffentlich bekannt. Auf einer kasachischen Telekommunikationskonferenz im Jahr 2022 erklärte ein Unternehmensvertreter vor laufender Kamera, das Unternehmen sei der „erste Vertreter der Firma NAG außerhalb Russlands“, und bestätigte damit, dass es sich nicht um einen unabhängigen kasachischen Vertriebspartner handelte. Es handelte sich vielmehr um einen Ableger eines russischen Netzwerks für Beschaffungen, das bereits vor den Sanktionen aufgebaut worden war, um die Einfuhr sensibler Güter aufrechtzuerhalten.

Fallstudie 2: Zwangsarbeit, militärische Endverwendung und staatliche Unternehmen in Deutschland

Der zweite Fall befasste sich mit strukturellen Risiken als mit Netzwerkrisiken, insbesondere mit Compliance-Risiken, die in Lieferketten verborgen sind, die auf Unternehmensebene auf den ersten Blick einwandfrei erscheinen. Ausgangspunkt ist ein italienischer Fertiger von Aluminium-Elektrolytkondensatoren mit einer Vertriebsniederlassung in Deutschland. Verfolgt man die Lieferkette drei Stufen zurück, ändert sich das Bild.

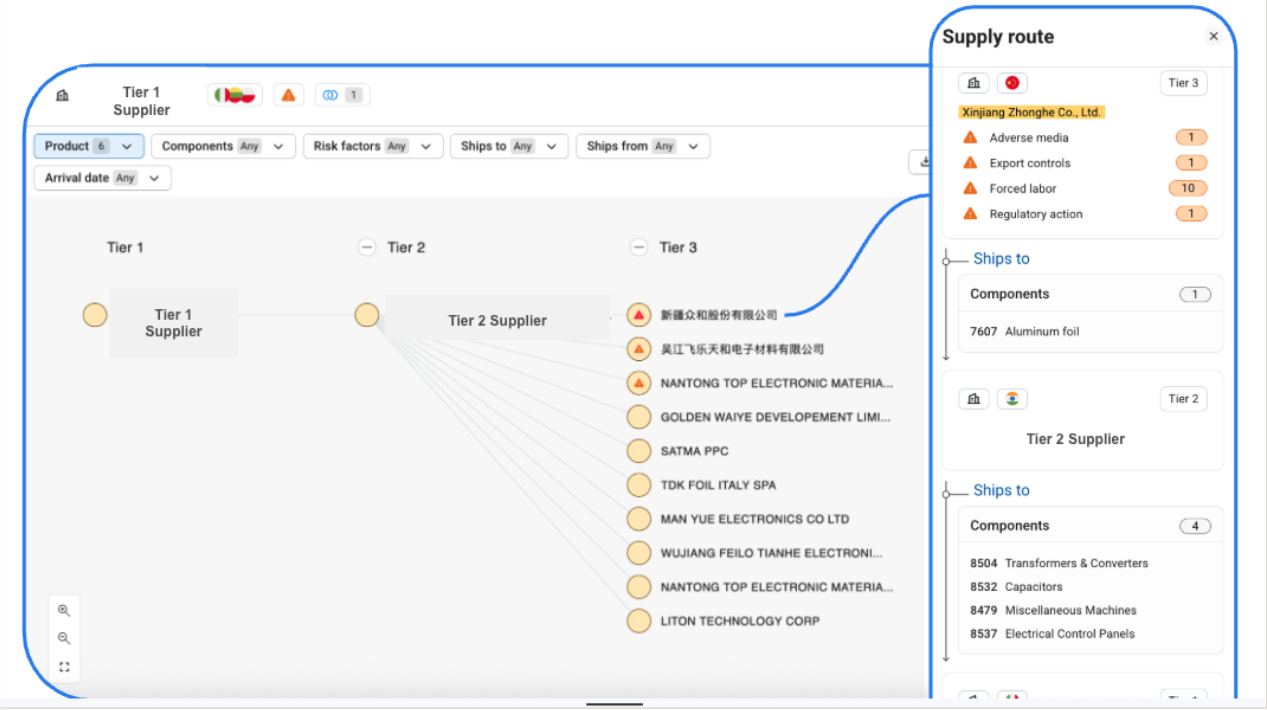

Abb. 3: Visualisierung der vorgelagerten Lieferkette eines italienischen Unternehmens mittels Sayari: Italien–Indien–Xinjiang

EBENE	LAND	ENTITÄT
TIER-1	**Italien**	Italienischer Fertiger. Screening auf Unternehmensebene zeigt keine Risiken.
TIER-2	**Indien**	Indische Produktionsgesellschaft. Beschafft Aluminiumfolien als Ausgangsmaterial.
TIER-3	**Xinjiang, China**	Xinjiang Joinworld (UFLPA-gelistet, Auftragnehmer der XPCC). In den italienischen Zollunterlagen sind 30

Dies ist in Zollfrachtbriefen dokumentiert und nicht nur eine Vermutung. In den italienischen Zollunterlagen sind z.B. 30 Direktlieferungen von einem von der US-Regierung als in Zwangsarbeit verwickelten Unternehmens verzeichnet. Bankbeziehungen, Akkreditive und Handelsfinanzierungen des Fertigers stehen u. U. in Verbindung mit dieser Lieferkette.

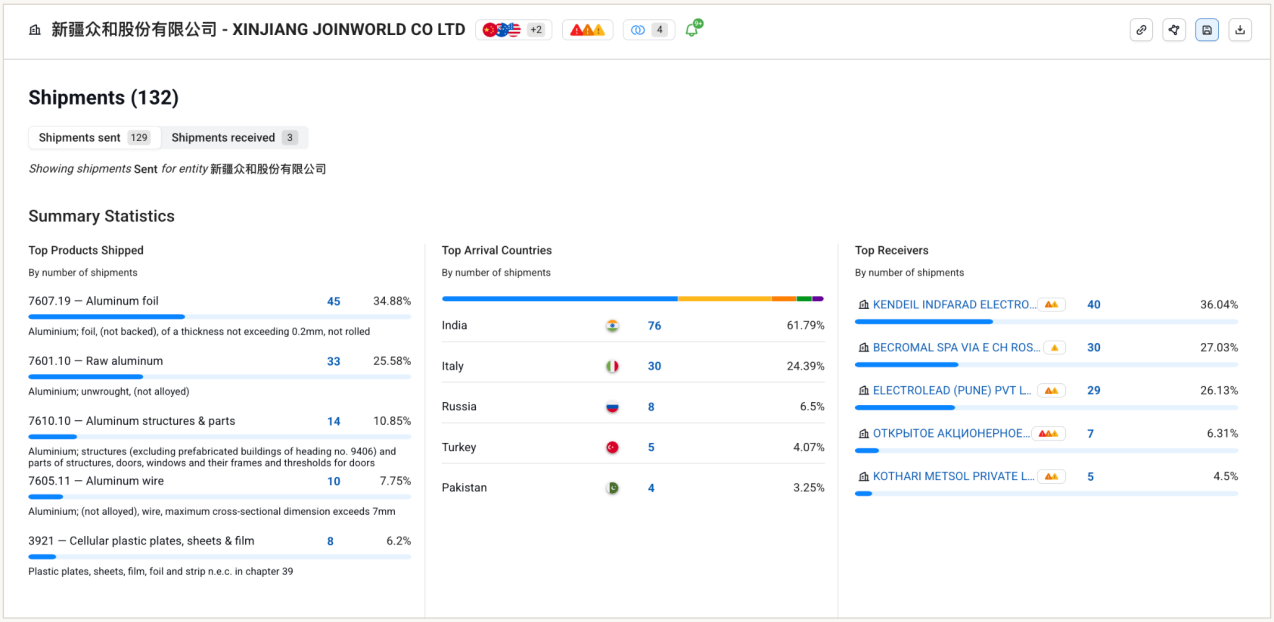

Abb. 4: Dokumentation der Handelsströme: von Xinjiang nach Italien

UFLPA

Die Beweislast

Der US Uyghur Forced Labor Prevention Act legt eine Presumption fest: Bei Waren von gelisteten Unternehmen wird davon ausgegangen, dass sie unter Einsatz von Zwangsarbeit hergestellt wurden, sofern der Importeur nichts Gegenteiliges nachweist. Für Banken, die diese Importe finanzieren, besteht ein direktes Compliance-Risiko. Die EU-Verordnung zur Bekämpfung von Zwangsarbeit (2024/3015), in Kraft seit Dezember 2024, sieht entsprechende Einfuhrverbote vor. Der Umbau der Due-Diligence-Prozesse dauert oft Jahre, d.h. die verbindliche Anwendung in der gesamten EU ab Dezember 2027 steht vor der Tür.

Auf Ebene der Tochtergesellschaften verschärft sich das Risiko noch weiter. Zum Unternehmensnetzwerk des börsennotierten Unternehmens aus Xinjiang gehören elf Tochtergesellschaften, die laut Sayari-Daten jeweils als Zwangsarbeitsrisiken eingestuft sind. Eine davon sticht jedoch aus einem Grund hervor. Ihre offizielle Gewerbeanmeldung, die bei

den chinesischen Behörden eingereicht wurde, gibt als Geschäftszweck unter anderem die Forschung und Entwicklung von Raketenstartanlagen sowie die Fertigung von militärischem Ausrüstungsmaterial an. Dies stammt nicht aus einem Geheimdienstbericht. Es handelt sich um Angaben, die das Unternehmen bei der chinesischen Regierung eingereicht hat und die alle von Sayari erfasst wurden, da das Unternehmen die Daten des chinesischen Unternehmensregisters direkt an der Quelle auswertet.

Die Eigentumsverhältnisse reichen von diesem Unternehmen über eine staatlich kontrollierte Provinzholding bis hin zur SASAC der Provinzregierung von Sichuan, einem Mechanismus, der letztlich mit dem chinesischen Staatsrat verbunden ist. Ein in der UFLPA-Liste aufgeführtes Unternehmen, das Zwangsarbeit einsetzt, hat eine Tochtergesellschaft, die für die Waffenherstellung registriert ist und vom chinesischen Staat kontrolliert wird. Diese ist Teil der Lieferkette von Unternehmen, die Geschäftsbeziehungen zu europäischen Banken unterhalten.

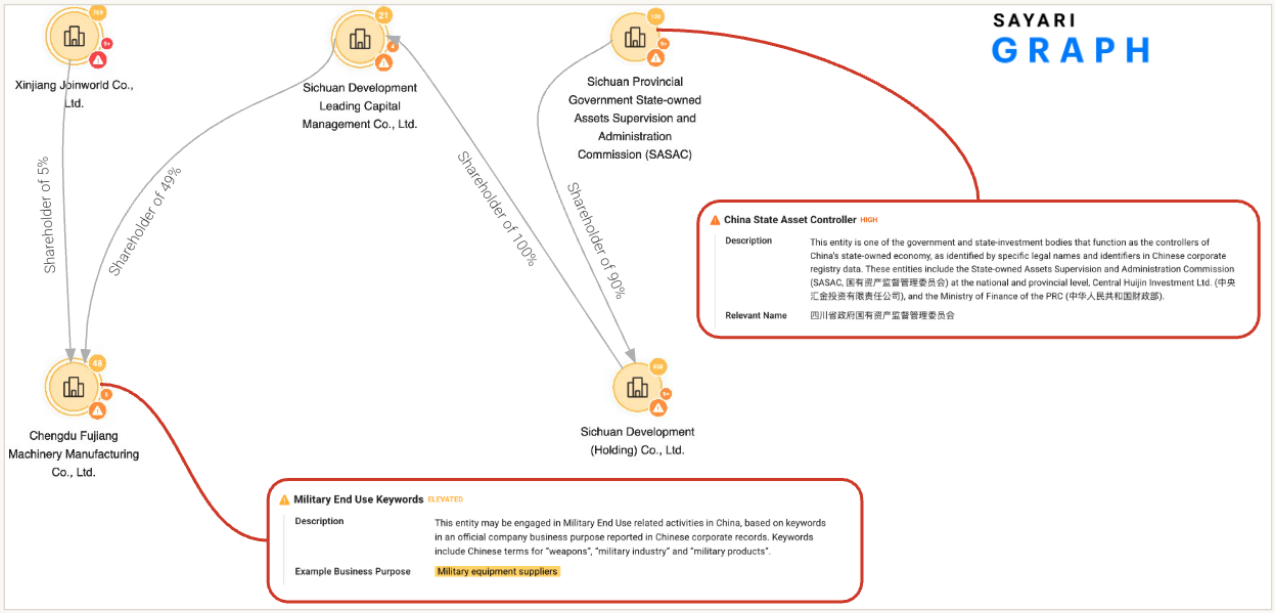

Abb. 5: Eigentumsverhältnisse: Unternehmen aus Xinjiang bis hin zum chinesischen Staat

CASIC

Im deutschen Handelsregister eingetragene Tochtergesellschaften

Die China Aerospace Science and Industry Corporation (CASIC) befindet sich zu 100 % in chinesischem Staatsbesitz und ist in der Liste des militärisch-industriellen Komplexes gemäß Abschnitt 1260 H des US NDAA aufgeführt. Sie ist zudem die wirtschaftlich Berechtigte von mindestens drei in Deutschland registrierten GmbHs, die von Sayari identifiziert wurden. Eine Standardabfrage im Handelsregister liefert deutsche Unternehmen. CASIC wird dabei nicht angezeigt. Dieser Zusammenhang wird erst durch registerlübergreifende Eigentumsverfolgung sichtbar: deutsche Eintragungen, die mit Daten staatlicher chinesischer Unternehmen verknüpft sind. Gemäß § 10 des Geldwäschegesetzes (GWG) ist eine verstärkte Sorgfaltspflicht erforderlich, wenn die Kette wirtschaftlich Berechtigter zu einem staatlich kontrollierten Unternehmen führt. Der Prüfungsschwerpunkt der BaFin umfasst chinesische Kundenportfolios. Die Diskrepanz zwischen den Ergebnissen einer standardmäßigen KYC-Prüfung und den tatsächlichen Daten ist nachprüfbar.

Beiden Fallstudien ist gemeinsam, dass das Risiko in den Daten liegt. Unternehmensregister verfügen darüber. Frachtbriefe nennen sie namentlich. Was bisher fehlte, war die Infrastruktur, um diese Quellen länderübergreifend miteinander zu verknüpfen, sowie die Ermittlungsdisziplin, um die daraus gewonnenen Erkenntnisse mit der Geschwindigkeit und in dem Umfang zu interpretieren, wie es die moderne Compliance erfordert.

DIE FRAGE, MIT DER JEDES GESPRÄCH ENDET

Wenn Prüfer fragen, wie Ihr Unternehmen wirtschaftlich Berechtigte ihrer chinesischen Kunden ermittelt hat oder wie Ihre Transaktionsüberwachung Zahlungen über Strohmänner aus der GUS für den Erwerb russischer Technologie aufgedeckt hat, wie lautet Ihre Antwort?

ÜBER SAYARI

Sayari ist die Entscheidungsinfrastruktur für vertrauenswürdige KI in den Bereichen Wirtschaftssicherheit und kommerzielle Risiken. Das „Sayari Commercial World Model“ wertet über 11 Milliarden Datensätze aus Primärquellen aus mehr als 250 Gerichtsbarkeiten aus und bildet damit die „Ground Truth“ des globalen Handels. Eine Entscheidungsontologie, in der über ein Jahrzehnt an Ermittlungserfahrung kodiert ist, und „Superconductor“, eine Plattform zur agentenbasierten Koordination, ermöglichen eine KI, die wie ein erfahrener Analyst argumentiert, ihre Arbeitsweise offenlegt und jede Erkenntnis bis zu ihrer Quelle zurückverfolgt. Sayari geniesst das Vertrauen der US-Zoll- und Grenzschutzbehörde, des US-Finanzministeriums und von Fortune-500-Unternehmen und wird von Tausenden Experten in über 35 Ländern eingesetzt, um Lieferketten zu sichern und illegale Netzwerke zu zerschlagen. Der Hauptsitz befindet sich in Washington, D.C.

sayari.com

HAFTUNGSAUSSCHLUSS