Observatoire ARGA

Report on Sanctions and Compliance for 2025

SANCTIONS ECOSYSTEM 3.0

Global Restructuring of Financial, Political and Compliance Control in the Era of the EU 20th Sanctions Package

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Division

Correspondence Address: 14 rue Jacques Laffitte, Bayonne, 64100

Contact: info@argaobservatory.org

Paris, 04 November 2025

Table of Contents

Executive Summary

The concept of "Sanctions Ecosystem 3.0" reflects a structural transformation of the global order in which sanctions are no longer a fragmented tool of foreign policy, but an embedded regulatory architecture. Sanctions cease to function as reactive measures and instead evolve into a permanent system of governance over capital, technology, raw materials, data flows and digital assets.

The EU 20th Sanctions Package against Russia is one of the clearest markers of this transition. It demonstrates a shift away from traditional sectoral restrictions toward a multi-layered, technology-driven, institutionally consolidated sanctions model. The regulatory focus is moving from individual entities to supply chains, logistical corridors, financial pathways, IT-infrastructure and technological accessibility of exported goods.

A new regulatory landscape emerges, defined by several core trends:

— Institutionalisation of sanctions: sanctions regimes become permanent elements of global governance, embedded into banking compliance, customs control, export regulation and corporate reporting frameworks.

— Deep integration of sanctions analytics into AML/KYC, export-control and corporate risk systems: sanctions-screening now operates alongside financial monitoring, while banks, fintech, logistics and trading entities must account for sanctions exposure at every stage of transaction flow.

— Globalisation of secondary sanctions: accountability expands beyond the jurisdictions of issuing states to include third-country actors, transit hubs, intermediaries, brokers, aggregators and digital platforms.

— Emergence of network-based regulatory control: oversight is shifting from targeted checks to ecosystem-level monitoring of supply chains, routing structures, brokerage layers, crypto platforms, cloud infrastructure and trade mediation channels.

The ARGA Observatory report analyses the architecture of the Sanctions Ecosystem 3.0 through the lens of the EU 20th package, assessing institutional, technological and political implications, along with exposure risks for:

— regulators,

— international banks and cross-border trade actors,

— logistics chains and intermediaries,

— sanctions-compliance research institutions,

— journalists, analysts and risk-intelligence groups.

This material is based on OSINT-research, EU regulatory documentation, compliance-framework analysis, sectoral datasets and expert-level interview inputs.

METHODOLOGY

The report is based on a multi-layer analytical model combining legal, economic, sanctions-regime and institutional research. The methodology integrates documentary sources, compliance practice, OSINT datasets and internal Observatoire ARGA analytical work.

1. Analysis of international sanctions frameworks

The research examines regulatory acts and sanctions packages including:

— **EU:** Council Decisions, Council Implementing Regulations, Delegated Acts, DG FISMA guidance documents;

— **US:** OFAC publications, Executive Orders, Directives, Compliance Notes;

— **UK:** UK Sanctions Regulations, OFSI Notices;

— **Canada, Australia, Japan:** official sanctions lists, regulatory guidance, export-control enforcement mechanisms.

Cross-jurisdiction differences, secondary-sanctions architecture and extraterritorial applicability were incorporated into comparative assessment.

2. Regulatory review and compliance-practice mapping

The report incorporates:

— OFAC risk-based compliance frameworks;

— EU due-diligence guidance for supply-chain screening;

— UK OFSI enforcement and circumvention-detection methodologies;

— internal regulatory manuals of Tier-1 banks and fintech institutions;

— sanctions-screening integration into KYC/AML systems.

Special focus was placed on sanctions integration into automated AML-monitoring environments.

3. Supply-chain and circumvention-route analytics (Eurasia, 2022–2025)

Data sources include:

— re-export of restricted goods through EAEU, Caucasus and Central Asia;

— identification of shadow logistics hubs;

— substitution of Western suppliers with Asia-based chains;

— multi-node transit structures involving Türkiye, UAE, China, Kazakhstan, Kyrgyzstan, Georgia.

The analysis draws on customs statistics, trade-tracking platforms, sector reports and OSINT monitoring.

4. International institutional datasets

Utilised sources include:

— Interpol on transnational finance structures;

— FATF on sanctions-evasion typologies and trade-finance exposure;

— OECD on supply-chain governance and transparency;

— UNODC on illicit technology transfer and shadow capital flows.

These datasets informed comparative and trend-based modelling.

5. ARGA Observatory research (2022–2025)

Integrated inputs from ARGA research on:

— transnational sanctions-evasion corridors,

— corporate disputes with sanctions components,

— abuse of AML/KYC and sanctions-coded rhetoric,

— EU/UK/CH/UAE banking-system responses to risk-origin jurisdictions.

More than **70 case studies** (public + NDA) were analysed, covering sanctions exposure, politically-driven investigations, freeze-actions and cross-border enforcement friction.

6. **Correlation of sanctions cases with corporate and political crises**

   A parallel analytical comparison was conducted between:

   — sanctions restrictions,

   — corporate conflicts and hostile takeovers,

   — nationalisation and pressure on asset holders,

   — political repression,

   — cross-border AML/sanctions signalling.

   This approach made it possible to trace hidden interdependencies between sanctions mechanisms and internal political–economic processes.

INTRODUCTION: SANCTIONS AS A NEW REGULATORY ARCHITECTURE

Modern sanctions have evolved beyond an instrument of foreign policy — they have formed a new multilayer global regulatory system in which political, legal, economic, technological and human-rights elements operate as a single mechanism. Sanctions now function as infrastructure that shapes international trade, digital security, global supply chains and corporate risk governance.

They have effectively become one of the key regulatory instruments of the 21st century — comparable in influence to international law, multilateral trade agreements and the Bretton Woods financial architecture.

Core functions of sanctions in the contemporary economy

1. Political function

Sanctions remain a tool of diplomatic leverage, but now operate within long-term strategic frameworks — from geopolitical containment to coalition-building. They are no longer tied to short episodic crises: sanctions have become a permanent feature of global political order.

2. Legal function

Sanctions generate enforceable norms recognised by courts and regulatory bodies. They expand the boundaries of both public and private international law. EU and US sanctions legislation increasingly serves as a source of mandatory compliance requirements for corporations worldwide.

3. Economic function

Sanctions act as a global filter governing access to capital, technology, finance and transport infrastructure. They redirect investment flows, reshape supply chains, influence asset valuation and redesign the architecture of global trade.

4. Technological function

Sanctions impose export and usage controls on critical technologies — from AI and microchips to satellite systems, cybersecurity and dual-use industrial components. For the first time in history, sanctions directly determine technological accessibility.

5. Compliance-regulatory function

Sanctions have become a foundation of corporate governance:

— sanction screening is embedded in KYC/AML,

— sanctions risk factors are incorporated into ESG and due diligence,

— export-control frameworks are converging with financial monitoring.

Banks and multinational corporations must maintain sanctions-compliance units, making sanctions a core pillar of global risk-management infrastructure.

6. Social and human-rights function

Sanctions operate as a mechanism for rights-based accountability:

they target corruption, electoral interference, transnational repression, and human-rights violations. Magnitsky-type regimes have created a new accountability standard across jurisdictions.

Sanctions 3.0 — The New Regulatory World Model

The emergence of the Sanctions Ecosystem 3.0 marks a transition to a regulatory paradigm in which sanctions perform political, legal and economic functions simultaneously, forming a unified institution of global governance.

This is the first system in history where:

— foreign-policy norms become mandatory for the private sector;

— restrictions operate transnationally, irrespective of jurisdiction;

— digital platforms, banks and logistics companies are forced to carry out regulatory functions;

— sanctions cease to be temporary measures and evolve into a long-term architecture of global flow governance.

The EU's 20th sanctions package is one of the clearest examples of this ecosystem, integrating financial, technological, legal and network-based instruments into a single control structure.

STRUCTURE OF THE SANCTIONS ECOSYSTEM 3.0

Global regulatory centres

Sanctions Ecosystem 3.0 forms around several major regulatory hubs that define compliance standards for the global financial and trade system. These centres not only issue sanctions legislation but possess the practical capacity to enforce compliance beyond their own borders.

The European Union

The EU is building the most comprehensive and legally consolidated framework. Its sanctions system is anchored in two interconnected instruments — Council Decisions (political-legal mandate) and Council Regulations (directly binding effect).

The EU is constructing a multi-layered regulatory web that embeds sanctions into financial compliance, export-control frameworks and internal corporate risk management.

The United States

The U.S. remains the dominant actor shaping global sanctions practice. OFAC maintains unparalleled extraterritorial reach due to the centrality of the U.S. dollar and American financial infrastructure.

Any entity interacting with USD, SWIFT or U.S. banking networks is effectively bound by U.S. sanctions — regardless of jurisdiction.

The United Kingdom

Following Brexit, the UK has become a highly agile sanctions authority. OFSI employs independent investigation mechanisms, penalty frameworks and regulatory guidance, making the British model more manoeuvrable than the EU but comparably influential.

Canada and Australia

Both states increasingly coordinate with the U.S. and EU, expanding Magnitsky-style regimes and framing common standards on corruption, human rights and cyber-security.

Japan and South Korea

These actors serve as technology-focused regulators, concentrating on semiconductors, electronics, defence industries and cyber-infrastructure. Their control lever makes Sanctions 3.0 particularly impactful on tech-import-dependent economies.

Singapore

Evolving into a new centre of compliance governance, Singapore is tightening supervision of financial flows and trade platforms, occupying the niche of an "Asian OFAC" — less politically driven but highly risk- and technology-oriented.

Collectively, these regulatory hubs form the core of the sanctions ecosystem — governing over 80% of global supply chains, banking operations and digital infrastructure.

3.2. Technological Restrictions

The key innovation of the Sanctions Ecosystem 3.0 is the extension of sanctions to high-tech sectors and digital infrastructure. Technological measures become an equivalent pillar of sanction policy alongside financial restrictions.

Export control gains exceptional significance. EU Regulation 2021/821 (Dual-Use Regulation) establishes a unified framework for controlling dual-use goods and technologies, including electronics, optics, satellite engineering, aerospace components and cyber-defence tools.

Sanctions now include:

• restrictions on the export of microchips, semiconductors and lithography equipment;

• prohibitions on transferring algorithms and technical documentation;

• bans on engineering, IT and consulting services related to high-tech production.

Artificial intelligence becomes a critical domain. For the first time, sanction regimes are being discussed for AI systems capable of autonomous malicious use — facial recognition, military simulation tools, intelligence platforms, UAV command systems.

Cybersecurity and spyware are also incorporated into the sanction perimeter. The EU and US impose restrictions on the export and servicing of spyware platforms, data interception systems and remote-access tools. Thus, sanctions begin regulating digital risk on the same level as physical goods.

Technological sanctions in Model 3.0 perform a strategic function: they do not merely punish — they control access to critical technologies that define global competition.

3.3. Secondary Sanctions

Secondary sanctions transform the sanctions system into a global enforcement mechanism extending beyond national jurisdictions.

This model introduces liability for third countries and companies even if they are not directly subject to primary restrictions.

Any company that:

• assists in sanction evasion,

• engages in re-export schemes,

• supplies equipment through intermediary chains,

may be classified as a violator and placed under restrictions.

A key feature is the "presumption of risk" principle. In some cases, a company is treated as high-risk not because it violated rules, but because it operates in a jurisdiction or with goods associated with sanction pressure.

The ban on re-export of sanctioned goods becomes central to the ecosystem — covering electronics, microchips, machining equipment, dual-use technologies, software and support services.

Secondary sanctions amplify the reach of Sanctions 3.0, making it globally enforceable regardless of a country's political alignment. As a result, even neutral states are forced to adjust their trade and financial practices to avoid falling under restrictions.

20th EU Sanctions Package: A New Regulatory Architecture

The 20th EU sanctions package against Russia represents a qualitative transition from targeted restrictions to a fully integrated regulatory system that no longer merely prohibits individual transactions, but restructures the entire infrastructure of global business, logistics, technology and compliance. The package stands as a peak in the evolution of the EU's sanctions regime, consolidating political, technological, financial and legal instruments into a unified framework.

1. Expansion of Dual-Use Goods Controls

The EU significantly broadens the categories of products previously viewed as strictly military-related. Now subject to control are:

• industrial microchips and electronic components,

• optical monitoring, navigation and positioning systems,

• data-processing equipment, servers, high-precision machining tools,

• materials and components used in UAV production,

• advanced sensors, integrated circuits, network communication devices.

The key shift is the EU's new view that any advanced technology may contribute to maintaining access to critical capabilities. Export control becomes a central pillar of the sanctions ecosystem.

2. Ban on High-End Services: IT, Marketing, Audit

For the first time, the EU introduces a comprehensive prohibition on intellectual and high-value professional services, previously minimally regulated:

• IT outsourcing and cloud computing services,

• marketing, consulting and analytical support,

• audit, accounting and corporate valuation,

• software development and technical maintenance.

This measure is one of the most consequential elements of the package. The EU recognizes that modern economies rely not only on goods, but on intangible expertise and access to global know-how. Denying such services effectively disconnects major Russian companies from international technological renewal, licensing and governance standards.

3. Blocking Intermediaries in Third Countries

A critical innovation is the built-in framework for monitoring circumvention hubs, including:

• UAE,

• Armenia,

• Kazakhstan,

• Turkey,

• Kyrgyzstan,

• Georgia.

For the first time, the EU introduces tools to sanction:

• intermediary companies,

• logistics hubs,

• re-export beneficiaries,

• entities involved in repackaging or diversion of goods.

This forms a secondary sanctions vertical that expands enforcement into jurisdictions outside the conflict. The EU effectively establishes a mechanism of transnational sanctions pressure analogous to U.S. OFAC secondary sanctions.

4. First-Ever Regulation of Crypto Infrastructure

For the first time in EU sanctions history, cryptocurrency infrastructure is placed under direct regulatory control, including:

• blocking digital wallets linked to sanctioned persons,

• bans on custodial wallet services,

• transaction oversight through EU-based crypto platforms,

• mandatory due-diligence for DeFi instruments operating within the EU.

This creates a precedent linking sanctions enforcement with digital-asset governance — extending regulation to stablecoins, mixers, DeFi protocols and NFT platforms.

5. Restrictions on Shipping and Insurance Services

Another cornerstone of the package is the new control framework over:

• maritime shipping operations,

• ship registry services,

• insurance and reinsurance,

• brokerage and chartering intermediaries,

• freight carriers and transport logistics firms.

The EU establishes a network-based oversight mechanism for global maritime supply chains, making the re-export of high-risk goods through intermediary states effectively impossible without exposing shipowners and carriers to sanctions risk.

6. Sanctions on Microchip & Electronics Supply Chains

For the first time, the package directly targets global suppliers — primary and secondary — of electronic components:

• manufacturers in East Asia,

• distributors in the UAE and Hong Kong,

• intermediary traders across Central Asia.

The EU gains the ability to restrict any company worldwide if it:

• supplies microchips to sanctioned entities,

• participates in circumvention schemes,

• violates export-control obligations.

This transforms sanctions into a *global technological filter* rather than a merely political instrument, shifting regulatory logic towards access-control over critical components.

7. Precedent Value of the 20th Package

The most important outcome is the establishment of a universal regulatory precedent: compliance must account for sanctions risk regardless of geography, supply route, or claimed neutrality of jurisdiction.

As a result, every nexus point in global trade becomes subject to sanctions screening:

• any intermediary,

• any distributor,

• any trading platform,

• any cryptocurrency exchange.

The 20th EU package formalizes the architectural shift to a model where sanctions operate as an integrated global infrastructure governing supply chains, technology circulation, financial transactions and digital asset flows.

GEOGRAPHY OF SANCTIONS EVASION: ARGA OBSERVATORY MAPPING

United Arab Emirates (UAE)

Primary global hub of parallel import & financial intermediation

The UAE remains the world's largest concentration point for companies involved in the re-export of high-tech products to Russia and other sanctioned destinations. Dubai, Ajman, Ras Al Khaimah and Sharjah function as distribution nodes for electronics, automotive components, telecommunications equipment, IT hardware and dual-use technology.

Infrastructure pillars:

• transit-layering firms with minimal physical footprint, specializing in multi-layer routing and invoice restructuring;

• OTC crypto-pools enabling large off-exchange USDT/USDC settlements outside Western visibility;

• re-import logistics built around Jebel Ali, Deira and Fujairah hubs;

• pseudo-distributors sourcing goods through Asian markets and relabelling them as unrelated imports.

The UAE's role is secured by a unique combination of developed logistics, light regulatory exposure, dense brokerage networks and political non-alignment with Western sanctions regimes.

Turkey — Caucasus — Central Asia

Macro-regional re-export network

Turkey operates one of the most influential alternative corridors for sanction-sensitive flows—especially electronics, CNC machinery, industrial components, aircraft parts and dual-use supplies.

Core mechanisms:

• Turkey → Caucasus → Russia: the dominant re-export triangle, relying on altered certificates of origin;

• EAEU logistics: Kazakhstan, Kyrgyzstan and Armenia serve as gateways to the EAEU customs zone, where traceability weakens significantly;

• customs-arbitrage strategies: tariff and certification asymmetries obscure routes of high-tech goods.

This corridor functions as a *Middle Belt of sanctions circumvention*, powered by tens of thousands of SME intermediaries.

Serbia & the Balkans

Politically neutral corridor outside EU regulatory perimeter

Serbia's non-EU status and geopolitical neutrality make it a strategic channel for companies seeking to bypass EU export control.

Key dynamics:

• Serbian firms appear in re-exports of electronics, optics and medical equipment;

• regional interlinkage through Bosnia & Herzegovina, Montenegro, North Macedonia;

• Balkan platforms are increasingly active in crypto-fintech operations bypassing EU oversight.

For Asian suppliers, the region is perceived as a *low-visibility entry point* into the European supply chain.

South Caucasus (Georgia — Armenia)

Fintech routing, crypto-clearance & IT-intermediation hub

The South Caucasus has emerged as a compact but highly technological zone of sanctions bypass, where the scale of flows is modest but sophistication is high.

Characteristic nodes:

• fintech firms operating PSP/EMI cross-border rails for CIS-based clients;

• crypto-gateways using stablecoins to settle high-tech equipment imports;

• IT intermediary companies shipping hardware and software as R&D or service-support assets.

Georgia and Armenia additionally serve as jurisdictions with access to platforms and payment railways no longer available inside the Russian market.

Asia (Hong Kong, Malaysia, Singapore)

Emerging centres of a new sanctions-shaping architecture

Hong Kong

Hong Kong acts as a global *proxy-hub* for Chinese industrial buyers, electronic component traders, optics manufacturers, server suppliers, telecommunications equipment and semiconductor logistics. Due to unique PRC–HK regulatory mechanics, the jurisdiction enables:

• origin-masking of exported goods,

• multi-layered corporate ownership stacks,

• large-value settlements in CNY and USDT.

Malaysia

Malaysia is rapidly becoming a hub for:

• semiconductors and IC assemblies,

• industrial and consumer electronics,

• security-systems hardware,

• high-volume re-export shipments via free-port infrastructure.

Singapore

Singapore represents an *emerging regulator*, building a hybrid model combining:

• ultra-strict compliance culture,

• deep digitalisation of export-control procedures,

• a growing re-export flow handled by private-sector brokers.

The Asian dynamic signals a shift from isolated intermediaries toward fully-formed *ecosystems of sanctions circumvention*, deeply integrated into global supply and value chains.

CLASSES OF ACTORS IN THE NEW SANCTIONS ECOSYSTEM

The emerging sanctions architecture produces its own ecosystem of participants — not only logistics intermediaries, but financial, technological and regulatory actors who now influence access to markets, supply chains, digital assets and banking infrastructure. ARGA Observatory identifies three core actor classes.

1. Sanctions Intermediaries

The core mechanical layer of Ecosystem 3.0

These are commercial structures that enable concealment of product origin, payment pathways, beneficial ownership and supply-chain continuity.

Sanctions intermediaries include:

• Operational Companies in UAE, Türkiye, Kazakhstan, Armenia

Used as façade-suppliers producing compliant-looking paperwork — invoices, certificates of origin, customs declarations — masking links to sanctioned jurisdictions.

• Logistics Hubs

Jebel Ali (UAE), Mersin (Türkiye), Poti (Georgia), Aktau (Kazakhstan), Limassol (Cyprus).

They allow multiple “re-threads” of the supply chain, changing packaging, HS codes, routing documents and origin labels.

• Origin-Hiding Brokers

Hybrid structures at the crossroads of trade & corporate services, issuing “clean invoices” and contractual chains concealing the true producer or end-recipient.

Function:

These actors *soften the rigidity* of sanctions infrastructure by creating alternative access corridors to global markets.

2. Corporate Sanction-Navigation Networks

Strategic architectures for long-range compliance circumvention

These are multi-jurisdictional legal & financial constructs involving companies, trusts, holdings and layered beneficiary networks.

Examples include:

• EU/Asian manufacturers using third-country routing

Electronics, optical systems, industrial hardware formally exported under compliance, but re-routed via intermediaries in UAE, Türkiye, China, Kazakhstan or Serbia.

• Purpose-built beneficiary networks for circumvention

Typically structured through:

– Hong Kong / Singapore holding shells

– BVI trusts and nominee boards

– proxy directors & multi-tier ownership configurations

• Split-chain corporate models

Company A delivers to a neutral jurisdiction → Company B re-exports into a sanctioned zone.

Function:

These networks make sanctions *legally enforceable yet practically navigable*, by redistributing risk across jurisdictions and actors.

Digital Intermediaries

Digital infrastructure has become a central operational layer of Sanctions Ecosystem 3.0 — a parallel financial universe enabling the coexistence of formal sanction controls and a shadow economy of digital assets.

Key vectors:

● P2P Platforms

Peer-to-peer environments facilitating direct exchange of cash, bank transfers and stablecoins without traditional financial institutions.

They create a *non-bank parallel financial network* operating beyond OFAC/OFSI oversight.

● Cryptocurrency Brokers

Specialized intermediaries performing:

• large-volume USDT/USDC conversion,

• obfuscation of asset provenance,

• transaction structuring designed to exit AML visibility windows.

They function as liquidity points that detach flows from traceable banking rails.

● Off-exchange OTC Pools

Closed-access liquidity channels often exceeding exchange-level daily volume.

They enable:

• trading without KYC,

• address-splitting and wallet proliferation,

• multi-hop “washing chains” for origin dilution.

Function:

Digital intermediaries form a *sanctions shadow layer* — an informal financial infrastructure enabling movement of capital, technology and services outside direct reach of Western regulators.

IMPACT OF SANCTIONS ON COMPLIANCE, DUE DILIGENCE & GLOBAL MARKETS

Sanctions-first Compliance Model — a structural shift

Between 2023–2025, sanctions compliance transitioned from a secondary security layer into the *primary decision-making mechanism* for global corporates. Banks, fintech providers, insurers, maritime operators and exporters now apply sanctions analysis *before* any standard risk review.

Structural Changes in Global Compliance Practice

• Country-Risk Banning

Major financial institutions increasingly impose outright prohibitions on servicing clients linked to:

Russia, Belarus, Iran, Syria, and selected Central Asian jurisdictions.

This has created restricted jurisdiction categories, where even lawful transactions require elevated justification and manual vetting.

• Expanded KYC & Sanctions-KYC 2.0

KYC evolves from identity verification into sanctions-oriented due diligence.

Standard requirements now include:

• full UBO transparency (100% disclosure),

• supply-chain mapping,

• sanctions-connectivity screening of counterparties,

• origin-of-funds verification through a sanctions-risk lens.

KYC becomes *a sanctions audit of the client* rather than a formal compliance step.

• Digital Asset Monitoring & Blockchain Intelligence

Banks and payment platforms integrate:

• on-chain analytics,

• link-analysis to sanctioned wallet clusters,

• surveillance of P2P/OTC liquidity routes,

• detection of "grey liquidity" pathways.

Chainalysis, TRM Labs, Elliptic and similar tools now operate as core infrastructure of global sanctions enforcement.

Sanctions scoring and sanctions-based credit risk

Companies and banks form a sanctions risk profile of a client based on:

• country of origin,

• type of business,

• sectoral exposure,

• digital footprint,

• payment geography,

• interaction with high-risk jurisdictions.

In a number of financial groups, sanctions scoring becomes a mandatory part of the client's overall credit rating.

Politicization of financial markets

Sanctions are reshaping the global financial system, making political context a key determinant of investment decisions.

• Cross-border trust degradation

Before 2022, trust between jurisdictions was based on banking standards and international law.

Now the decisive elements are:

• the geopolitical positioning of a state,

• its level of sanctions exposure,

• its alignment within international alliances.

This creates a sanctions-based geography of trust where countries are informally divided into:

• “safe” for capital (EU, US, UK, JP, KR, SG),

• “complex” (Kazakhstan, Kyrgyzstan, Georgia, UAE),

• “excluded” (Russia, Belarus, Iran, Syria).

• Financial markets become political arbiters

Major exchanges, clearing systems, banks and crypto-providers are forced to:

• refuse clients from politically sensitive regions,

• conduct sanctions audits of companies and funds,

• assess risk based not only on financial but also political criteria.

• Changing trajectories of investment and capital

Investors are reducing their presence in countries with high sanctions exposure.

Capital inflows into Eurasia are shrinking, while:

• capital relocation to the UAE and Singapore increases,

• shadow-banking expands across Central Asia,

• private equity and venture capital become increasingly politicized.

• Fragmentation of the global economy

Sanctions form a dual-contour world system:

1. The Western sanctions contour (EU–US–UK–JP–KR–SG) — high compliance standards.
2. The parallel contour (UAE–Turkey–Central Asia–China) — flexible circumvention mechanisms.

   Financial markets cease to function as a single global space, evolving into a network of differentiated access zones with varying levels of systemic risk.

EXAMPLES FROM PRACTICE

Case 1 — Turkey → Armenia → Russia

Mechanism: simplified customs + origin substitution + electronics re-export.

This corridor is used to bypass EU and U.S. export controls on dual-use goods such as microchips, industrial machinery, and telecommunications equipment. The pattern involves:

• initial export from Turkey classified as "general industrial equipment";

• re-declaration in Armenia, where the product receives a new HS code and "new" country of origin;

• re-export to Russia as Armenian or Turkish-origin goods.

The scheme relies on shell-type companies with 1–2 employees and minimal warehousing. Its advantage is simple customs clearance and absence of supply-chain verification. The downside is a high probability of detection through insurance records, CMRS tracking, and logistics metadata.

Case 2 — UAE → Kazakhstan → Russia

Mechanism: grey logistics brokers + nonlinear routing + repackaging.

The UAE is one of the largest global hubs for parallel imports. The scheme operates through:

• purchase of electronics, auto-parts, machinery and IT hardware via Dubai-based trading firms;

• shipment to Kazakhstan under the cover of EAEU-destined imports;

• repackaging and relabeling within logistics hubs in Almaty and Astana;

• re-export to Russia with no traceable direct link to the UAE or the EU.

A typical enhancement is the use of nonlinear routing, e.g.:

UAE → India → Azerbaijan → Kazakhstan → Russia

or

UAE → Uzbekistan → Kazakhstan → Russia.

Such "route noise" disrupts the origin trail and lowers the probability of falling under OFAC/EU control.

Case 3 — Georgia → Lithuania (cryptocurrency)

Mechanism: USDT transit via OTC pools + mixing + pseudobanking.

Used to bypass financial sanctions and banking transfer restrictions. The flow generally looks like this:

1. A Russian client sends USDT to a large OTC broker in Tbilisi.
2. The broker mixes funds off-chain, breaking the link to incoming wallet addresses.
3. Assets move through multiple transit wallets owned by different platforms.
4. On the EU side (commonly Lithuania, Estonia, or Germany), funds are processed via a fintech platform as *merchant payments* or *P2P settlements*.
5. The final balance is credited to a bank account as "income from cryptocurrency trading."

This channel constitutes what ARGA defines as pseudobanking — a para-banking system based on crypto-settlements yet embedded inside European fintech infrastructure.

RISKS AND CHALLENGES

The modern Sanctions Ecosystem 3.0 generates a complex landscape of threats for international markets, regulators and business. The expansion of the sanctions infrastructure is accompanied by the emergence of grey zones, the growing politicization of financial processes, and an increasing burden on global oversight mechanisms.

1. Expansion of grey zones and parallel supply chains

The growth of restrictions stimulates non-linear logistics routing, the use of intermediaries in Turkey, the UAE, Kazakhstan, Georgia and Serbia, and the spread of multi-layered re-export schemes. This reduces trade transparency, complicates export-control verification, and increases the likelihood of sanctioned goods entering sensitive sectors. Grey zones create a parallel economy that generates strategic risks for the EU and the U.S., undermining sanctions efficiency.

2. Overload of international mechanisms, including Interpol

Sanctions-related cases are increasingly accompanied by Interpol requests, overloading Diffusion and Blue Notice channels. Several states have begun using these instruments to exert pressure on emigrants, investors and business migrants. This creates a risk of declining trust in international criminal-notice systems and increases the volume of politically motivated requests that require filtering.

3. Emergence of pseudo-compliance (fake compliance)

Corporate structures and intermediaries are developing formal-looking compliance frameworks that imitate adherence to sanctions while enabling circumvention. This includes "clean" invoices, falsified certificates of origin, fragmented supply chains and multi-layer payment structures. Pseudo-compliance produces an appearance of legitimacy while facilitating sanction evasion. For banks, it increases KYC/EDD workload and creates a need for technical document auditing.

4. Growth of politically motivated financial investigations

In several CIS states, sanctions discourse, AML tools and FIU requests are used as pressure mechanisms against NGOs, media, independent business figures and political opponents. These investigations increasingly stretch across borders through FIU channels, banks and digital platforms. This erodes confidence in international information-exchange frameworks and exposes new risks for refugees, emigrants and civil-society actors.

5. Deterioration of the business environment in Eastern Europe and the post-Soviet region

Sanction-related risks, politicized compliance checks and closure of financial channels are driving reduction in foreign investment, rising transaction costs and the exit of international companies. A "sanctions-fragmented" landscape is emerging, in which certain states lose access to global capital markets while domestic firms are forced into expensive workaround schemes. Long-term implications include deindustrialization and declining competitiveness.

RISK MAP

Country	Risk Level	Key Threats	Abuse Triggers	Transnational Effect
Russia	**CRITICAL**	Politicized AML; AML+Interpol coupling; mass freezes; pressure on business emigrants	"Foreign agent" status; economic predicates without damage	Freeze in EU/UK/CH; Interpol abuse; offboarding
Kazakhstan	**VERY HIGH**	Corporate AML; blanket FIU requests; freeze-before-investigation	Corporate disputes; asset redistribution	Freeze in EU/CH/UAE; grey logistics schemes
Azerbaijan	**VERY HIGH**	AML-based targeting of journalists & NGOs; currency/tax predicates	Human rights activity; media work	Cross-border freezes (Turkey, Georgia, EU)
Turkmenistan	**VERY HIGH**	Opaque FIU; nationality-based blocking	Any external business activity	Automatic KYC refusal in EU/UK/UAE
Uzbekistan	**HIGH**	Elite conflicts; FIU without evidence; diaspora pressure	Large assets; family holdings	Freeze in UAE/Turkey/EU
Belarus	**HIGH**	AML used in political cases; sanction shadowing	Protest activity	Freeze in EU/UK; bank offboarding
Tajikistan	**HIGH**	FIU under security control; "extremism" predicates	Diaspora; religious & business activity	Freezes in Turkey/EU; bank refusals
Kyrgyzstan	**MEDIUM**	AML vs NGOs & journalists; partial politicization	Media, investigations, grant-funded organizations	Temporary freezes; localized FIU alerts
Georgia	**MEDIUM**	AML in "foreign influence" cases; crypto channels	Journalists, activists	USDT corridors → EU; fintech risks

Country	Risk Level	Key Threats	Abuse Triggers	Transnational Effect
Moldova	**MEDIUM**	Corporate & politico-economic freezes	Corporate conflicts	Episodic transnational signals
Armenia	**MEDIUM–LOW**	Tax/corporate freezes; crypto-linked vulnerabilities	Holdings, IT sector	Crypto channels → EU; P2P risk vectors

FORECAST 2025–2027

ARGA Observatory anticipates a continued strengthening of global sanctions architecture and further consolidation of the Sanctions Ecosystem 3.0. Secondary sanctions are expected to become the primary enforcement mechanism targeting states that continue to facilitate circumvention channels — with the most significant impact projected for the UAE, Turkey, Kazakhstan, and Armenia.

Simultaneously, regulatory pressure on crypto-infrastructure will intensify: authorities will move toward sanctions-based oversight of OTC platforms, P2P markets, informal brokers, and mandatory monitoring of on-chain transaction flows.

Sanctions are likely to become more geographically distributed: Asia and the Middle East will form their own regulatory hubs, producing a layered system of sanction regimes. Export control will tighten across electronics, AI, semiconductors, aviation, and high-tech manufacturing.

Finally, Interpol abuse risks will increase — several states may weaponize sanctions terminology to target opponents and business abroad, necessitating more stringent filtering of politically motivated notices.

RECOMMENDATIONS

For international institutions:

• establish a global sanctions-risk indicator;

• integrate monitoring of digital assets (OTC, P2P, mixers, stablecoins);

• enhance oversight of grey logistics & fintech hubs (UAE, Turkey, Caucasus, Central Asia);

• standardize FIU data exchange for circumvention routes;

• introduce early-warning systems for cross-border circumvention schemes.

For the EU & the United States:

• expand supply-chain control, including multi-layered transit paths;

• create a registry of high-risk intermediaries (logistics, trade, crypto-services);

• implement sanctions stress-tests for corporations;

• restrict access to critical technologies through secondary sanctions;

• strengthen export-control enforcement in electronics, AI, chips, and aviation sectors.

For academic institutions:

• develop sanctionology as a new interdisciplinary field;

• build datasets of circumvention routes, intermediaries, and case studies;

• publish updated cartographic research on sanctions supply-chains;

• increase collaboration across economics, law, political science, and cyber-security disciplines;

• advance modelling of the Sanctions Ecosystem 3.0.

CONCLUSION

The Sanctions Ecosystem 3.0 represents a profound transformation of the global order — one in which sanctions are no longer a temporary measure, but a stable norm of international regulation. They cease to be a reactive tool and instead become a structural component of global governance, comparable in significance to international law, trade frameworks, and financial supervision systems.

This new model builds its own institutions, channels of influence, technical protocols, and actors — from state regulators to digital platforms and transnational intermediaries. Sanctions evolve into a multi-layered infrastructure that governs access to capital, technology, logistics, digital assets, and global trust networks.

Within this landscape, the role of independent analytical bodies increases dramatically. ARGA Observatory is forming a new school of sanctions analytics, integrating political science, international law, economics, criminology, financial-flow research, and digital-security studies.

Our mission is to produce objective, methodologically grounded insight into the sanctions environment, identify transnational risks, develop forward-looking policy models, and strengthen the global legal framework.

The development of sanctions analytics is no longer merely a research discipline — it is a contribution to building a transparent, predictable, and secure international order.

SOURCES

1. FATF, Anti-Money Laudering and counter-terrorist financing measures, Qatar, Mutual Evaluation Report, May 2023, https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Qatar-2023.pdf.coredownload.inline.pdf.
2. Freedom House, Still Not Safe : Transnational Repression in 2022, Yana Gorokhovskaia, Nate Schenkkan, and Grady Vaughan, April 2023,

https://freedomhouse.org/sites/default/files/2023-04/FH_TransnationalRepression2023_0.pdf.
3. FATF, Anti-Money laundering and counter-terrorist financing measures, Luxembourg, Mutual Evaluation Report, September 2023, https://www.fatf-gafi.org/en/publications/Mutualevaluations/MER-Luxembourg-2023.html.